2006-03

Operation of long-haul non-LOS wireless tactical networks

Zachariadis, Christoforos P.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OPERATION OF LONG-HAUL NON-LOS WIRELESS TACTICAL NETWORKS

by

Christoforos Zachariadis

March 2006

Thesis Advisor:	Alex Bordetsky
Second Reader:	Carl Oros

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Operation of Long-haul Non-LOS Wireless Tactical Networks			**5. FUNDING NUMBERS**
6. AUTHOR Christoforos Zachariadis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The IEEE 802.16-2004 wireless standard is a robust, wireless, longhaul solution for connecting remotely located, forward operating bases. Proof of concept for this capability is the NPS OFDM testbed for the research and support of the communications and collaborative processes between tactical operators within a wireless network. This thesis will attempt to develop strategies for implementing network management, establish a performance baseline for the NPS testbed and define the acceptable metrics for QoS.

Field experimentation scenarios, network performance management tools and modeling tools are the techniques that we are using to assess the operation of 802.16 NPS testbed for its quality requirements. A baseline is conducted to record the state of the network operation and investigate the operational guidelines and conditions for the network to support collaborative applications. The baseline provides good organization, status monitoring and planning capabilities that will help in troubleshooting future failures. Using OPNET Modeler ACE we examine the network traffic flow and diagnose performance issues for critical applications. Finally, we develop appropriate policies to fine-tune network behavior within a holistic ad hoc collaborative environment.

14. SUBJECT TERMS Tactical Network Topology, IEEE 802.16, Network Management, Fixed Wireless Broadband Access, Collaborative Environment, Situational Awareness.			**15. NUMBER OF PAGES** 105
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OPERATION OF LONG-HAUL NON-LOS WIRELESS TACTICAL NETWORKS

Christoforos P. Zachariadis
Major, Hellenic Army
B.S., Hellenic Army Military Academy, 1986

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT
and
MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2006

Author: Christoforos Zachariadis

Approved by: Alex Bordetsky
Thesis Advisor

Carl Oros
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The IEEE 802.16-2004 wireless standard is a robust, wireless, longhaul solution for connecting remotely located, forward operating bases. Proof of concept for this capability is the NPS OFDM testbed for the research and support of the communications and collaborative processes between tactical operators within a wireless network. This thesis will attempt to develop strategies for implementing network management, establish a performance baseline for the NPS testbed and define the acceptable metrics for QoS.

Field experimentation scenarios, network performance management tools and modeling tools are the techniques that we are using to assess the operation of 802.16 NPS testbed for its quality requirements. A baseline is conducted to record the state of the network operation and investigate the operational guidelines and conditions for the network to support collaborative applications. The baseline provides good organization, status monitoring and planning capabilities that will help in troubleshooting future failures. Using OPNET Modeler ACE we examine the network traffic flow and diagnose performance issues for critical applications. Finally, we develop appropriate policies to fine-tune network behavior within a holistic ad hoc collaborative environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

AN-50e	Redline Communications' system
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CENETIX	Center for Network Innovation and Experimentation
CDMA	Code Division Multiple Access
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
DoD	Department of Defense
dB	Decibel
dBi	db referenced to an isotropic antenna
DSL	Digital Subscriber Loop
DSSS	Direct Sequence Spread Spectrum
EIRP	Effective Isotropic Radiated Power
FBWA	Fixed Broadband Wireless Access
GIG	Global Information Grid
GHz	Gigahertz
GUI	Graphical User Interface
HVT	High Value Target
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical
Kbps	Kilobits Per Second
LAN	Local Area Network
LLNL	Lawrence Livermore National Lab
LOS	Line of Sight
LRV	Light Reconnaissance Vehicle

MAC	Media Access Control
MAN	Metropolitan Area Network
MIB	Management Information Base
MOUT	Military Operations in Urban Terrain
NBFC	National Biometrics Fusion Center
NCW	Network Centric Warfare
NLOS	Non-line-of-sight
NOC	Network Operations Center
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PMP	Point-to-Multipoint
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
QoS	Quality of Service
RF	Radio Frequency
SA	Situational Awareness
SINADR	Signal to Noise and Distortion Rate
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
TNT	Tactical Network Topology
TOC	Tactical Operations Center
UAV	Unmanned Aerial Vehicle
USSOCOM	United States Special Operations Command
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area network
WiMAX	Worldwide Interoperability for Microwave Access

ACKNOWLEDGMENTS

I would like to express my greatest appreciation and gratitude to my thesis advisor Dr. Alex Bordetsky, for his continuous guidance and mentorship. I feel lucky to have been one of his students and part of CENETIX. Also I would like to express my deepest thanks to Carl Oros, Eugene Bourakov, and Mike Clement for their assistance and support in my thesis work.

Lastly and above all, I will be forever thankful to my loving wife, Maria, and our two daughters, Amalia and Dimitra, for their continued love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Information superiority plays a critical role in determining a decisive victory in the current warfare and asymmetric threats. Improvements in communication infrastructure, in terms of higher bandwidth backbone and Quality of Service (QoS) support, are necessary for enhancing war fighting capabilities. The complexity of networking architectures, the use of collaborative technologies and the real-time monitoring of the battlefield have contributed to the development of different levels of decision makers in the Global Information Grid (GIG). According to National Security Agency (NSA) the objective of the GIG is:

> The Global Information Grid (GIG) will be a net-centric system operating in a global context to provide processing, storage, management, and transport of information to support all Department of Defense (DoD), national security and related Intelligence Community missions and functions - strategic, operational, tactical, and business – in war, in crisis, and in peace. GIG capabilities will be available from all operating locations: bases, posts, camps, stations, facilities, mobile platforms, and deployed sites. The overarching objective of the GIG vision is to provide the National Command Authority (NCA), war fighters, DoD personnel, Intelligence community with information superiority, decisions superiority, and full spectrum dominance.

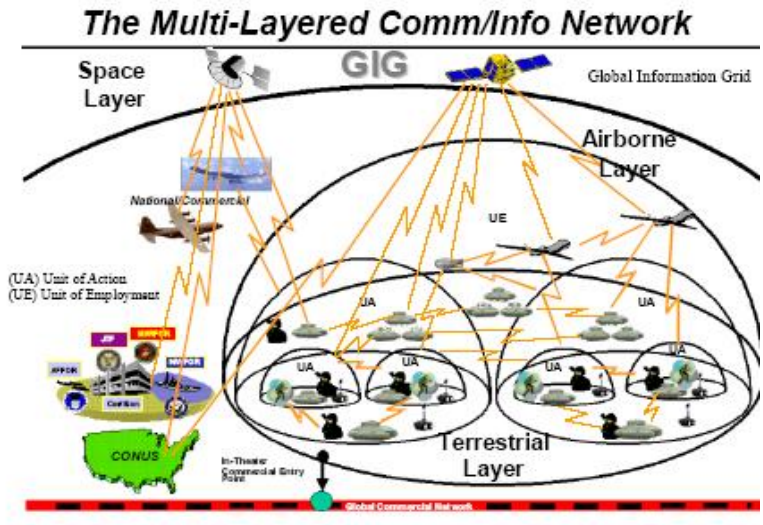


Figure 1. The Global Information Grid (From: US Army CONOPS for Network Centric Signal Support)

This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. With command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) becoming one of the most important elements of military operations, the technology should be flexible and reliable enough to provide war fighters and decision makers with the right information at the right time.

The goal is to increase the net-centricity of war fighters, by enabling increased reach among the GIG users, increased adaptability of information to operational needs, and increased network awareness. Network awareness refers to the effects of operational feedback provided to the war fighters and back to the decision makers, and how this feedback on the status of the network will enable users to organize their own behavior (Bordetsky et al).

The National Association for Amateur Radio (ARES) describes a number of desirable characteristics of a rapid deployment network for emergency responses and continuity of information flow, in case of disaster. The network should:

- Provide rapid transfer of emergency traffic
- Provide flexible access between sections
- Be automated as much as practical
- Use available and future digital modes
- Interface with commercial communication systems, such as conventional and cellular telephone and the Internet
- Have speed, performance, and accuracy
- Provide immediate traffic delivery

Combining the aforementioned sources and in order to maintain all the above facets of information exchange in the highly mobile, rapidly changing battlefield, the decision support systems will depend heavily on advanced wireless communications. One of the major challenges in deploying the GIG is to expand to the tactical level and provide the management architecture for it.

1. Expanding GIG to the Tactical Level: 802.16 OFDM Solutions

Information should be delivered from the last mile to the Global Information Grid (GIG) and to the decision makers through high speed backbone networks. Currently, optical cables are used for the high speed network backbone. The 802.16 OFDM broadband wireless access system is a promising technology for interconnecting the last mile information environment to the GIG meeting accurate and real-time needs for war fighters as well as high bandwidth and QoS in military networks. The deployment of a broadband wireless Wide Area Network (WAN) has many advantages in contrast to the wired networks:

- Low cost
- Fast deployment speed
- Network architecture flexibility
- Network independence

The major advantage of the wireless networks is that they can support the dynamic nature of military missions, which require mobility and highly adaptive ad-hoc organization.

Figure 2 is an example of a tactical network, depicting the last mile command and control communication infrastructure using different wireless technologies. On the move, front line forces are equipped with wireless mesh technology. They communicate with the base command (TOC- Tactical Operation Center) using different alternatives and information travels through a high speed wireless connection to the Network Operation Center (NOC).

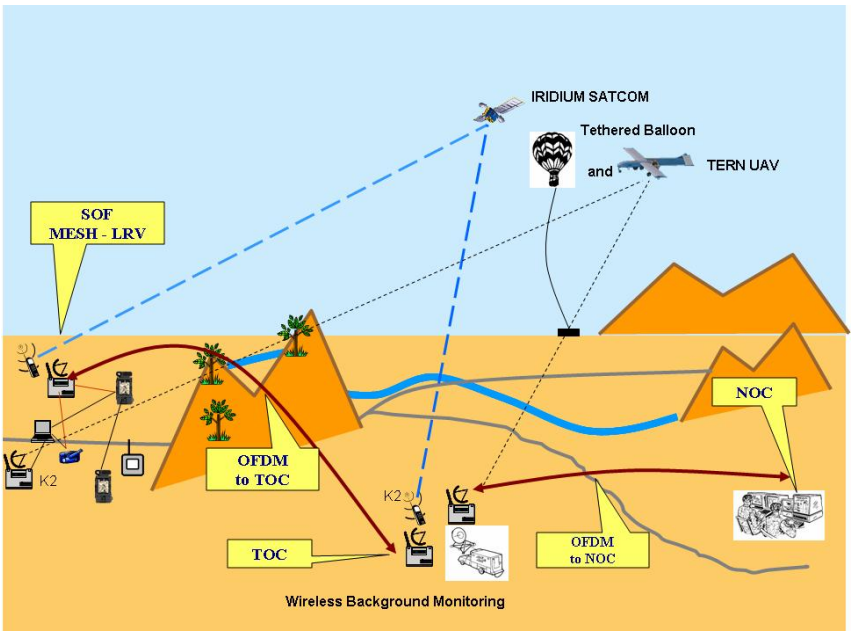


Figure 2. Surveillance and Target Acquisition Network (After: STAN, NPS-CENETIX)

2. Network Management Challenges

a. Existing Approach in Management Services

The grid is an integrated environment of different networking platforms, converging technologies, applications, and distributed decision makers. Effectively managing the network complexity and information infrastructure, across functional areas within their own boundaries, is the most demanding task. Figure 3 depicts the network management layer as an integral part of the GIG systems reference model.

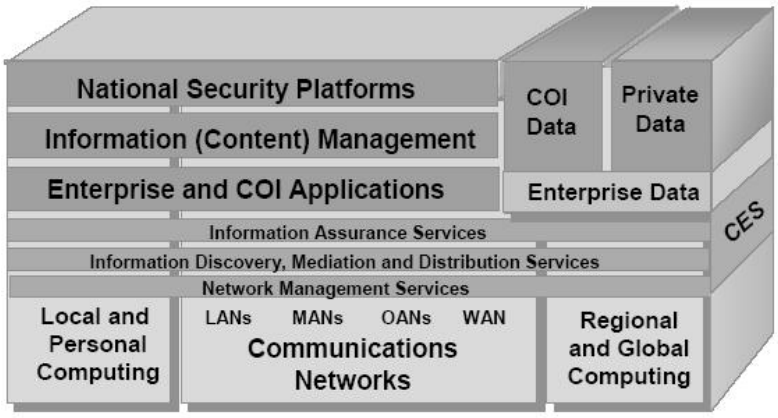


Figure 3. GIG Systems reference Model (From: Osterholz, DoD CIO)

At the tactical level, the Tactical Operations Center (TOC) oversees and guides the mission requirements of the ground combat operations. On the top level, the NOC facilitates the communication channels between the TOC and the mobile ground forces, connects them to the GIG and provides feedback to the last mile users, thereby improving operations. This makes the NOC the basic unit of grid management and the most important in tactical networks.

A variety of military applications and collaboration tools that are used in tactical networks require QoS support, in terms of delay and bandwidth utilization. Failed or diminished use of military critical applications in tactical networks, as well as poor management of network elements, carries a high cost to war fighting capabilities.

In order to successfully manage a tactical network's performance, NOC personnel should be equipped with certain information about the network behavior. This knowledge of network behavior patterns requires continuous and successful monitoring of the network, by using real-time statistical analysis and graphical reports.

The element that ties all the network characteristics together and supports the key information processing tasks that make a tactical network run effectively is performed by the Network Management System (NMS).

b. Managing Tactical Extensions

In the 21st century battlefield, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) are the most important elements of military operations.

The development of a flexible and reliable Tactical Network Topology (TNT) of manned/unmanned sensors and vehicles will network war fighters and decision makers and will improve operations by providing the right information at the right time.

The goal of network centric warfare is to support operations with an adaptable, mobile network capable of increasing the reach among users in a tactical environment, the adaptability of information to operational needs, and network awareness, which is the operational feedback provided to war fighters and back to the decision makers.

Integrating information from a large number of dynamically changing, collaborative agents and accurately monitoring the network, are the most important challenges for managing TNT extensions. Since the primary focus of war fighters is to accomplish their mission, the NOC is responsible for managing and controlling the information systems in the tactical network.

3. NPS Testbed for Exploring GIG Tactical Extensions

The Center for Network Innovation and Experimentation (CENETIX) headed by Naval Postgraduate School professor Dr. Alex Bordetsky, is the vehicle for exploring GIG tactical extensions, integration and operation. It is an ongoing research effort to explore new technologies for mobile, last mile communications, in support of Special Operation Forces (SOF) and provides a field experimentation capability that permits the United States Special Operations Command (USSOCOM) to rapidly address challenges facing deployed forces.

The NPS field experimentation program began three years ago with the purpose of providing the opportunity for students and faculty to evaluate some of the latest technologies and network configurations in an operational environment and measure the network performance and effectiveness.

A long-haul 802.16 OFDM fixed backbone wireless link extends for over 120 miles using a point–to-point architecture, connecting laboratories at NPS campus; NPS beach; and a UAV test facility at the California Army National Guard, Camp Roberts, CA. Figure 4, shows the wireless NPS long-haul testbed.

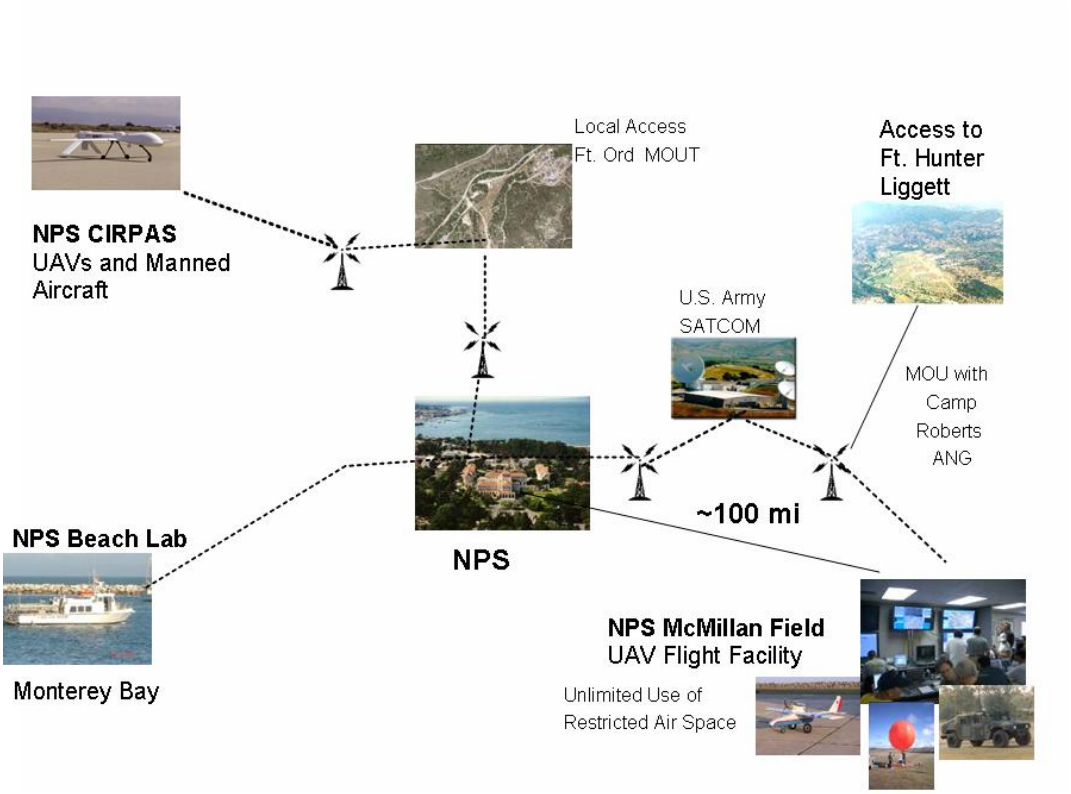


Figure 4. NPS 802.16 OFDM Fixed Backbone

Network management is accomplished by two network operations centers, one at NPS and the other at Camp Roberts. The last one serves as a TOC and operates only during experiments.

The main NOC at NPS is operated by faculty and thesis students and is responsible for monitoring the health of the network 24/7, and collecting observational data and statistics for future reference. From the NPS NOC the network facilitator or watch officer improves network operations, coordinates efforts and resources, and maintains network awareness providing feedback to all of the participants on the status of the network. A detailed description about the NOC's network operation functions are presented in the following chapters.

B. OBJECTIVES

The primary objective of this study is to examine in detail the performance of the wireless 802.16 OFDM testbed at NPS. The current approach involves measurements of existing systems and field experiments with different wireless technologies and collaborative applications.

The ultimate objective is to identify performance metrics and establish a baseline for the network administrator in order to be able to isolate problems and indicate performance issues. The emergence and use of collaborative technologies and the Peer-to-Peer (P2P) traffic consumes enormous volumes of bandwidth. In addition, wireless networks perform differently from the corresponding wired ones. This study will attempt to determine the acceptable performance metrics for critical network nodes and applications. Establishing a baseline and having the knowledge of the network behavior in different situations is very beneficial for planning new technologies and applications.

Finally, this study explores the operational requirements and the management functions that are administered by the NPS NOC. It attempts to chart a path for effective network management, maintaining network awareness and using the three levels of the network management system (NMS): performance management, configuration management, and fault management.

C. RESEARCH TASKS

The first questions are in regards to the network performance: what are the traffic behavior patterns across the network? What actions should be taken by the NOC to optimize network activity and avoid network congestion? In order to answer these questions it is necessary to:

- Identify performance metrics
- Identify running applications
- Interview the participants (stakeholders) to determine end-user requirements

- Use network management tools to collect data
- Analyze data

The second question is about the role and the organization of the NPS NOC in providing feedback to different wireless users. An analytical description is presented, concerning the responsibilities as well as the diagnostic tools for effectively monitoring the status of the network by the NPS NOC.

D. SCOPE

The main focus of the study is to measure the performance of the NPS long haul wireless OFDM 802.16 testbed during TNT experiments using available software tools and testing new wireless technologies and collaborative applications. In addition, this thesis will be focused on the functions that should be performed by the NOC to optimize network activity.

E. METHODOLOGY

- Identify network performance metrics
- Apply Network Management tools and develop procedures for configuration, monitoring and performance management. Tools that we are going to use are: Solar Winds Engineers Edition, Solar Winds Orion, OpManager and Ethereal
- Collect and analyze data from normal traffic as well as field experimentation during TNT experiments at Camp Roberts
- Analyze application transactions from TNT testbed and diagnose performance issues and network anomalies in traffic flows using OPNET Application Characterization Environment™ (ACE)

F. THESIS ORGANIZATION

This thesis is organized as follows: Chapter II compares different wireless technologies and describes the design of an 802.16 OFDM fixed broadband wireless

system. Chapter III provides details about network management and addresses the responsibilities of the NOC. Chapter IV proposes a network management plan, describes the NPS infrastructure, and contacts a network baseline. Chapter V describes an operational scenario using advanced networking and collaborative technologies and compares the network behavior to the baseline. Chapter VI covers a short description of OPNET Modeler ACE and the modeling of the TNT environment during TNT 06-1. Chapter VII includes our final conclusions and recommendations for future research.

II. APPLICABILITY OF WIRELESS TECHNOLOGIES FOR TACTICAL EXTENSIONS

A. WIRELESS EVOLUTION

Broadband is a term that has been used in various ways throughout the communications history. Broadband is considered any communication technology that provides high-speed data transmissions, with 1.5 megabits per second (Mbps) being widely used as a threshold. Sweeney (2004, 1) states that “the term wireless broadband generally refers to high-speed (minimally, several hundred kilobits per second) data transmissions occurring within an infrastructure of fixed points.”

Currently, cable and DSL are the dominant broadband access services in the marketplace. Practical limitations in features and deployment have prevented them from reaching many potential broadband Internet customers, and a large number of areas throughout the world are not able to access broadband connectivity. The most prevalent reason is that wired broadband connection is an expensive process. DSL can only reach about 3 miles from the central office switch, many older cable networks have not been equipped to offer a return channel, and converting these networks to support high-speed broadband can be very expensive.

Sweeney (2004) and Ibe (2002) describe various technologies that have been used for to deliver wireless broadband to the “last mile,” as a lower cost alternative to cable and DSL, or to provide backhaul for WLANs, such as WiMAX, Satellite, and Smart Antennas to name a few.

Wireless broadband can offer the solution to what is called the "last mile" problem, in places like remote geographical areas and rural areas with low population density. Even in those places where wired technologies can be deployed, it is always easier to set up a fixed wireless access network (Ibe, 2002). The following table summarizes the main differences between wired and wireless networks.

Network Characteristic	Wired Network	Wireless Network
1. Visual determination of network connectivity	If you can see the network cable going to a location, that location can be connected to the network.	Wireless networks sometimes connect locations that you cannot visibly see.
2. Visibility node-to-node on the same network	All of the nodes on a wired network can hear all other nodes.	Many nodes on a wireless network cannot hear all of the other wireless nodes on the same network.
3. Visibility network-to network	Wired networks are invisible to other wired networks. The presence of one wired network has no effect on the performance of another wired network.	Wireless networks are often visible to other wireless networks. One wireless network can affect the performance of other wireless networks.
4. Atmospheric properties	Performance is not affected by the properties of the atmosphere.	Performance can be affected by the properties of the atmosphere.
5. Terrain properties	Performance is not affected by the properties of the earth's terrain.	Performance is strongly affected by the properties of the earth's terrain.
6. User connectivity and mobility	Connectivity is possible only to physical locations to where the network cabling extends.	Connectivity is possible beyond the bounds of physical network cabling.

Table 1. Differences Between Wired and Wireless Networks (From: Unger, 2003)

B. WIRELESS STANDARDS

The area of Wireless technology has grown rapidly in recent years and various standards have come up in the last four years, as shown in Figure 5. Each of the wireless standards has a unique set of advantages and disadvantages in terms of mobility, range,

bandwidth and interference. There is a whole range of commercially available systems from IEEE802.11 standard offering up to 2 Mbps, to the Ultra Wideband (UWB) technology which aims to provide transmissions up to 450 Mbps.

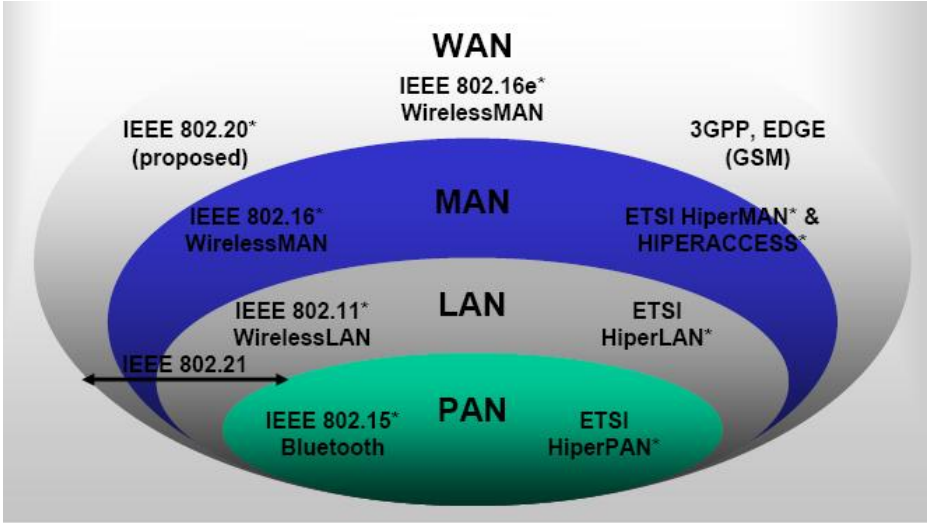


Figure 5. Wireless Standards (From: WiMAX Forum)

1. Overview of the IEEE 802.11 Standard

The 802.11 standard has gone through many iterations and expansions over the years and it is the first standard deployed for public short-range wireless networks. Gast (2005, 13) identifies the 802.11 family, also known as Wi-Fi, that is an IEEE certified wireless networking standard and currently includes the IEEE 802.11a, 802.11b and 802.11g specifications.

The 802.11b specifies Direct Sequence Spread Spectrum (DSSS) systems that operate at 1, 2, 5.5 and 11 Mbps transmission of data in the 2.4 GHz industrial, scientific, and medical (ISM) band. The 802.11a, describes wireless LAN device operation in 5GHz Unlicensed National Information Infrastructure (UNII) band, using Orthogonal Frequency Division Multiplexing (OFDM) technology and data rates up to 54 Mbps. The 802.11g specification also uses OFDM and provides the same maximum speed as 802.11a but operates in the 2.4 GHz ISM band. It features complete backwards compatibility with 802.11b devices.

802.11 has become a de facto standard because it is inexpensive, dependable and operates in a freely available unlicensed spectrum. However, it was never designed for Metropolitan Area Network (MAN) deployment. The solution to this problem was given by the 802.16 standard, which is designed to cover large areas.

2. Overview of the IEEE 802.16 Standard

The IEEE 802.16 Working Group in Broadband Wireless Access was originally organized to establish standards for fixed broadband systems operating above 11 GHz. The committee work was expanded to include systems operating on frequencies from 2 to 11 GHz which is designated as IEEE 802.16a. The 802.16a standard for the 2 to 11 GHz frequencies uses the same medium access control layer (MAC) as 802.16, but has different components in the physical layer because of the different frequencies covered. The 802.16 states a maximum throughput rate of 124 Mbps and the 802.16a standard a maximum of 70 Mbps for a 20 MHz channel bandwidth.

a. IEEE 802.16-2004 Std

The IEEE Standard for Local and Metropolitan Area Networks - Part 16 “Air Interface for Fixed Broadband Wireless Access Systems”, revises and consolidates IEEE Std 802.16-2001, IEEE Std 802.16a-2003 and IEEE Std 802.16c-2002 (IEEE, http://www.ieee802.org/16/pubs/80216-2004.html). This standard specifies the air interface of fixed broadband wireless access (BWA) systems supporting multimedia services. The MAC supports a primarily point-to-multipoint architecture, with an optional mesh topology (IEEE 802.16-2004). The MAC is structured to support multiple physical layer (PHY) specifications, each suited to a particular operational environment. For operational frequencies from 10-66 GHz, the PHY is based on single-carrier modulation. For frequencies below 11 GHz, where propagation without a direct line of sight must be accommodated, three alternatives are provided: Orthogonal Frequency Division Multiplexing (OFDM), Orthogonal Frequency Division Multiple Access (OFDMA), and single-carrier modulation (IEEE 802.16-2004).

b. Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a multicarrier transmission technique, which permits radios to operate better in multipath environments as well as to retrieve weak signals in marginal settings. Because OFDM is made up of many narrowband tones, narrowband interference will degrade only a small portion of the signal and has no or little effect on the remainder of the frequency components (Cisco). A message is assigned to a number of narrowband subcarriers simultaneously. The specified number of subcarriers for 802.16a, is 256.

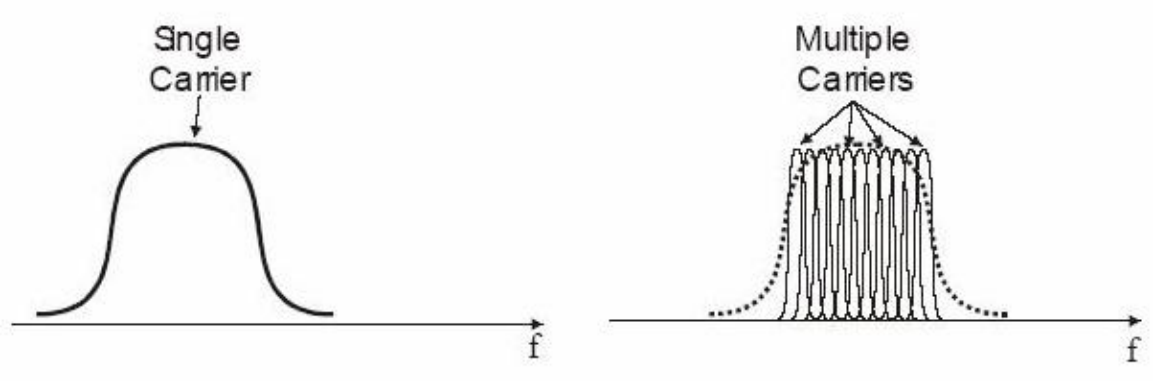


Figure 6. OFDM Signal Diagram (From: Redline, 2003)

c. Multipath Distortion

Anderson (2003, 369) and Sweeney (2004, 40) describe multipath distortion, or multipath fades, as the condition where the received signal is a combination of a primary signal and several echoed signals due to reflections along the path. The reflections converge out of phase with the directly received signal, causing variations in the amplitude of the signal at the receiver.

d. WiMAX

Worldwide Interoperability for Microwave Access (WiMAX) is the organization who tests and certifies products for interoperability and enforces compliance to the standard (Sweeney 2004, 5). Organizations are getting together to test their implementations against each other. They try to achieve interoperability by removing any ambiguities in the standards at an early stage. Equipment that have been approved as certified, can use the "WiMAX CERTIFIED" text and logo.

C. COMPARISON BETWEEN 802.11 AND 802.16 STANDARDS

All wireless standards have as their goal an acceptable performance level and the achievement of full interoperability among the products of standards-compliant manufacturers. The final choice depends on the operational requirements. The following table summarizes the major differences between 802.11 and 802.16 standards.

	802.11	802.16
Range	Optimized for users within 100m radius Add Access Points or high gain antenna for greater coverage	Optimized for typical cell size of 7-10 km Up to 50 km range No hidden node problem
Coverage	Optimized for indoor environments	Optimized for outdoor environments Support for advanced antenna techniques and mesh
Scalability	Channel bandwidth for 20 MHz is fixed	Channel bandwidth is flexible from 1.5 MHz to 20 MHz for both licensed and licensed exempt bands Frequency re-use Enables cell planning for commercial service providers
Bit Rate	2.7 bps/Hz peak data rate; up to 54 Mbps in 20 MHz channel	3.8 bps/Hz peak data rate; up to 75 Mbps in a 20 MHz 5 bps/Hz bit rate; 100 Mbps in 20 MHz channel
QoS	No QoS supporting today - 802.11e is working to standardize	QoS designed in for voice/video, differentiated services

Table 2. Wireless Standards comparison (From: WiMAX FORUM)

D. FIXED BROADBAND WIRELESS SYSTEMS

With the term “fixed” we mean that the transmitting and receiving terminals of the microwave link system remain at the same location, like terminals mounted on towers, or attached to the ground, or some other structure (Anderson, 2003).

The 5.8 U-NII band is frequently assigned to backhaul and offers bandwidth at 100 MHz and more than 20 miles range. Ibe (2002, 3) highlights the fact that fixed broadband wireless access networks have several advantages over any other alternative solution such as xDSL, cable, fiber optic and direct broadcast satellite. Rural areas with

low population density, remote geographical areas, and urban areas with old communication infrastructure are good candidates for fixed wireless broadband access.

Fixed broadband wireless systems operate in the 2.0 to 2.7 GHz, 3.5 to 3.7 GHz, and 5.1 to 5.8 GHz frequency ranges, when the transmitter and receiver are non-line-of-sight (NLOS). NLOS is a term which refers to any technique that minimizes the effects of physical obstructions. Because no NLOS technique can entirely eliminate the effects of blockage, the success can be measured in terms of the received signal strength (Sweeney, 2004).

1. Types of Fixed Wireless Networks

Anderson (2003, 17) states that the types of fixed wireless network topologies fall into four broad categories:

a. Point-to-Point (PTP) Networks

Point-to-Point (PTP) network links are connected end to end, use highly directional antennas and can span great distances. They are usually used to provide backhaul from a central office (NOC) to a remote location. Figure 7 illustrates a PTP network connecting two remote sites through mountaintop repeaters.

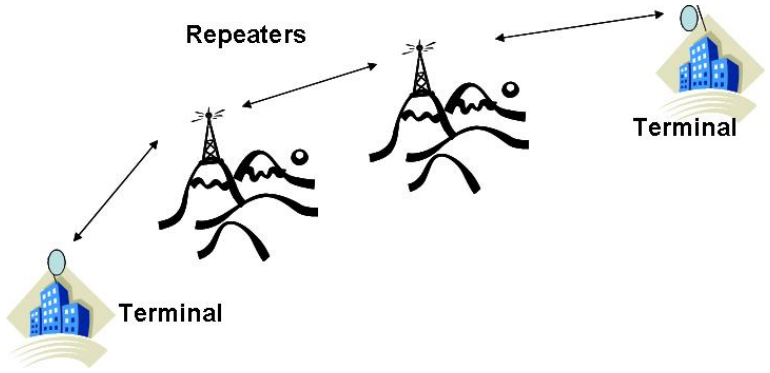


Figure 7. Point-to-Point (PTP) network (After: Anderson, 2004)

b. Consecutive Point and Mesh Networks

Consecutive Point networks (CPN) consist of a number of links that are connected end to end and configured as rings. They are usually attached to an optical fiber node at some point along the ring. The data traffic travels in both directions around the ring, so if a problem develops at some point, data traffic is not interrupted. Consecutive point networks are implemented for connecting buildings within a city,

using repeaters on the roofs of the buildings. Mesh networks are connected in both rings and branching structures. It is the most expensive architecture, because each node requires a router. They provide alternate paths usually for customers who lack line-of-sight.

c. Point-to-Multipoint (PMP) Network

Point-to-multipoint (PMP) fixed wireless topology which utilizes low microwave frequencies is the most popular construction. There is a hub approach analogous to the base station in a cellular system. One or more highly directional parabolic dishes, which are known as sectoral antennas, radiate from the base station towards multiple subscribers installed in LOS locations.

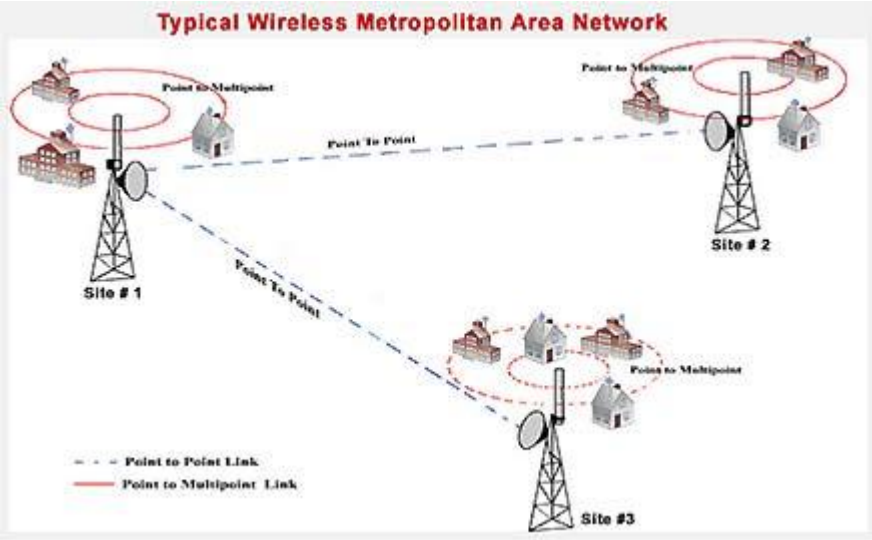


Figure 8. Point-to-Multipoint (PMP) Network (From: Cisco)

d. NLOS Point-to-Multipoint Networks

The only difference from the PMP networks described above is that, in most cases, the remote terminals do not have a clear view of the base station.

2. Fixed Wireless Link Design Considerations

Wireless communication systems certainly have many advantages over the wired networks, but meeting performance goals and service objectives is not a straightforward case. Below is a brief description of some very important issues that the wireless network operator should take in consideration:

a. Propagation Models

Wireless communication between two fixed points requires consideration of some critical factors that affect the electromagnetic (EM) propagation and determine how the wireless link will perform. For this purpose, propagation models are the fundamental tools for predicting system performance and what will happen to the transmitted signal on its way to the receiver. These models use detailed terrain databases and fading conditions, to determine whether the system meets its performance objectives successfully. Hills, mountains, buildings and other features can block and severely attenuate radio signals. They may also reflect and scatter the transmitted signals creating multiple paths of propagation. The effectiveness of the wireless system depends on the accuracy of the models, including terrain, building, and atmospheric databases that describe the propagation environment. Anderson (2004) provides an analytical description of the propagation models and how they are used in designing fixed wireless systems.

b. Fresnel Zones

One of the fundamental design objectives is to achieve adequate path clearance for the link. This means that every point on the path between transmit and receive antennas has a certain distance from any obstacles along the path. Anderson (2004, 35) refers to Fresnel zone as a 3-dimensional ellipsoid around the path with largest width in the middle of the path. The design objective for an LOS is to adjust the transmitting and receiving antennas in such a way so the 0.6 first Fresnel zone is free from obstructions. Increasing the antenna heights is the best way to accomplish adequate clearance. Digital elevation models (DEM) are used to create a terrain profile and take into account different weighting factors that may affect the wireless system. Figure 9 shows a terrain profile along an identical radio path, derived from OPNET, illustrating the path clearance between two points of the NPS wireless backbone.

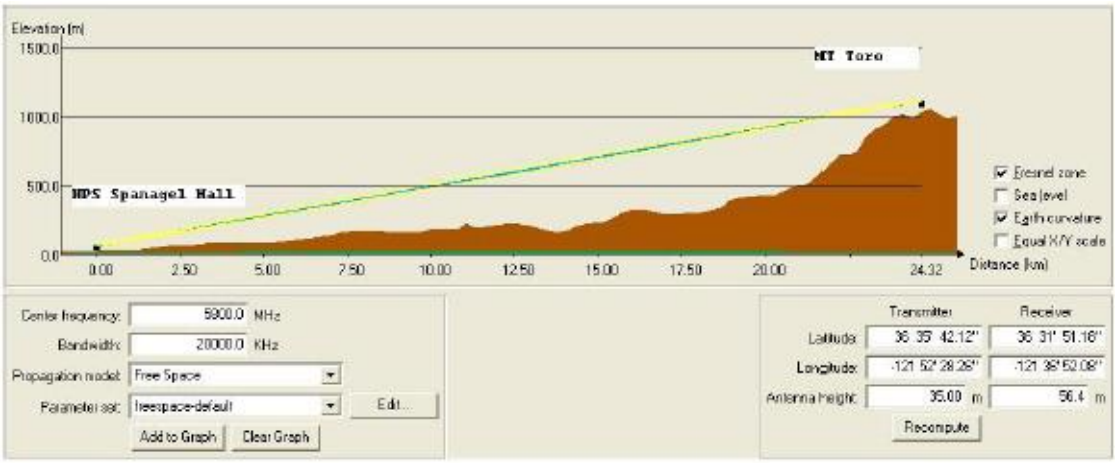


Figure 9. Terrain Profile (From: NPS- CENETIX)

c. Site Surveys

Site survey is an ongoing process for every link in the backbone, to determine the interference levels, the severity of obstructions and multipath at the locations where we want to install the terminals. Multiple measurements are taken to determine signal strength, bit error rate, jitter, latency and throughput.

d. Antenna Systems

For PTP systems the objective is to send the transmitted signal towards the receiver, so very highly directional antennas are needed. Unlike mobile systems the antenna polarization can be exploited to increase the capacity of the system. Use of adaptive antennas, who respond to the changing characteristics of the propagation environment, can increase the efficiency of the wireless system (Anderson, 2004).

III WIRELESS NETWORK MANAGEMENT

A. BACKGROUND IN NETWORK MANAGEMENT

Networks and distributed processing systems have become critical factors in the business world. Companies and organizations develop large and complex networks with an increasing number of applications and users. As networks become larger and more complex, tools and applications to ease network management are critical. Only a well-planned network can deal with changes effectively and efficiency. Poor network performance has a significant impact on an organization's productivity, especially in Tactical Networks where fast and reliable data transfer is needed. Every day network administrators face various problems and questions that need to be addressed. Questions concerning the network performance are:

- Where is the network slow?
- What applications are consuming the most bandwidth?
- Are all the links function properly?
- What are the proper thresholds for critical nodes to be monitored?
- Which interfaces are dropping the most packets?

All the above questions have one answer: Only proper management planning and proactive management detect problems before they escalate.

1. Functional Areas of Network Management

Network management is the ability to monitor, control and collect statistics on the state of the network from a central location. The International Standards Organization (ISO) has defined a conceptual model that classifies network management into five submodels. Subramanian (2000, 135) describes the functionality for each one of them:

a. Fault Management

Provides functions to discover faults in network operation determine the cause of the problem and perform corrective action.

b. Configuration Management

Addresses the settings for monitoring the network configuration information. Also deals with the reconfiguration, initialization and updating of network nodes.

c. Performance Management

Provides functions to evaluate the behavior and effectiveness of the network elements, as well as to gauge the utilization and performance of network devices and gather statistical data about the system.

d. Accounting Management

Measures the network utilization and the cost for such use by individual users or groups. It provides facilities for billing information and keeps network performance at an acceptable level by detecting inefficient use of the network (Ibe, 2002).

e. Security Management

Provides functions for protecting network resources from unauthorized users and provides notifications for security issues.

This thesis will examine the first three functional areas of network management for the NPS Tactical Network testbed.

2. Network Management Architecture

The network management architecture is generally the same in all network management systems and consists of the following building blocks as shown in Figure 10.

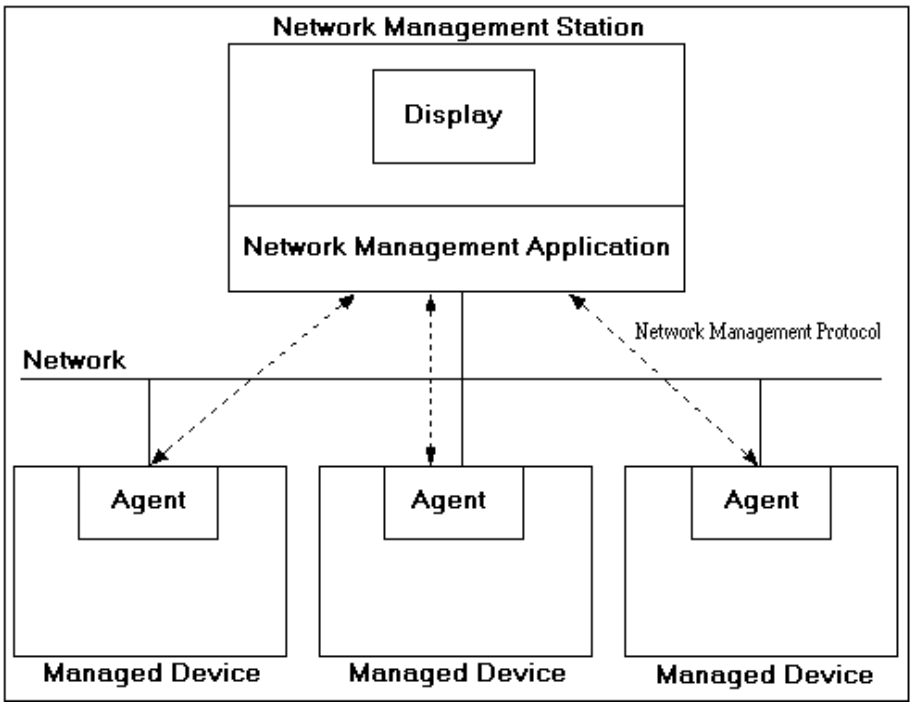


Figure 10. Typical Network Management Architecture (From: Cisco.com)

a. Network Management Station

The network management station is responsible for running the management applications that monitor and control the managed objects. It has a GUI interface which allows the operator to view a graphical representation of the network, control the network elements and sometimes react to information or thresholds from managed objects.

b. Managed Object

The managed object is a physical device (such as a computer, printer, router or an access point) or a logical resource (such as an application) whose performance level we need to monitor.

c. Management Agents

Managed agents are the software that reside in a managed object and provide information about the managed device to the network. This software accepts control information and is responsible for sending alarms to network management stations.

d. Network Management Protocol

The network management protocol is the protocol that is used by the management application and the agent to exchange information. The most commonly used protocol is the Simple Network Management Protocol (SNMP), which is designed for TCP/IP networks.

e. Management Information Base (MIB)

The MIB is a database that contains hierarchically organized information about the attributes of the managed objects and basically allows the monitoring and control of a managed device. “The MIB contains the name, object identifier (a numeric value), data type and indication of whether the value associated with the object can be read from and/or written to. A network management station monitors network elements by reading the values in the MIB,” (www.networkworld.com). The common structures for the definition of management information used in managing TCP/IP networks are included in the Structure of Management Information (SMI). SMI describes the object information model, which is used to organize, describe and name objects for the purpose of management so that information can be retrievable and modifiable by the SNMP. A MIB object is one of the specific characteristics of a managed device. Managed objects are comprised of one or more object instances (variables) and they can be found in two types: scalar and tabular. Scalar objects define a single object instance and tabular define multiple related object instances.

The MIB hierarchy can be depicted as a tree, as shown in Figure 11 that groups MIB objects and uses an abstract syntax notation to define manageable objects. “Each item on the tree is assigned a number (shown in parentheses after each item), which creates the path to objects in the MIB. This path of numbers is called the object identifier (OID). Each object is unique and it is identified by the path of numeric values,” (www.3com). The object identifier is the sequence of integers, separated by periods that can be obtained by enumerating the nodes that lie on the path from the root of the tree to the node where the object is located.

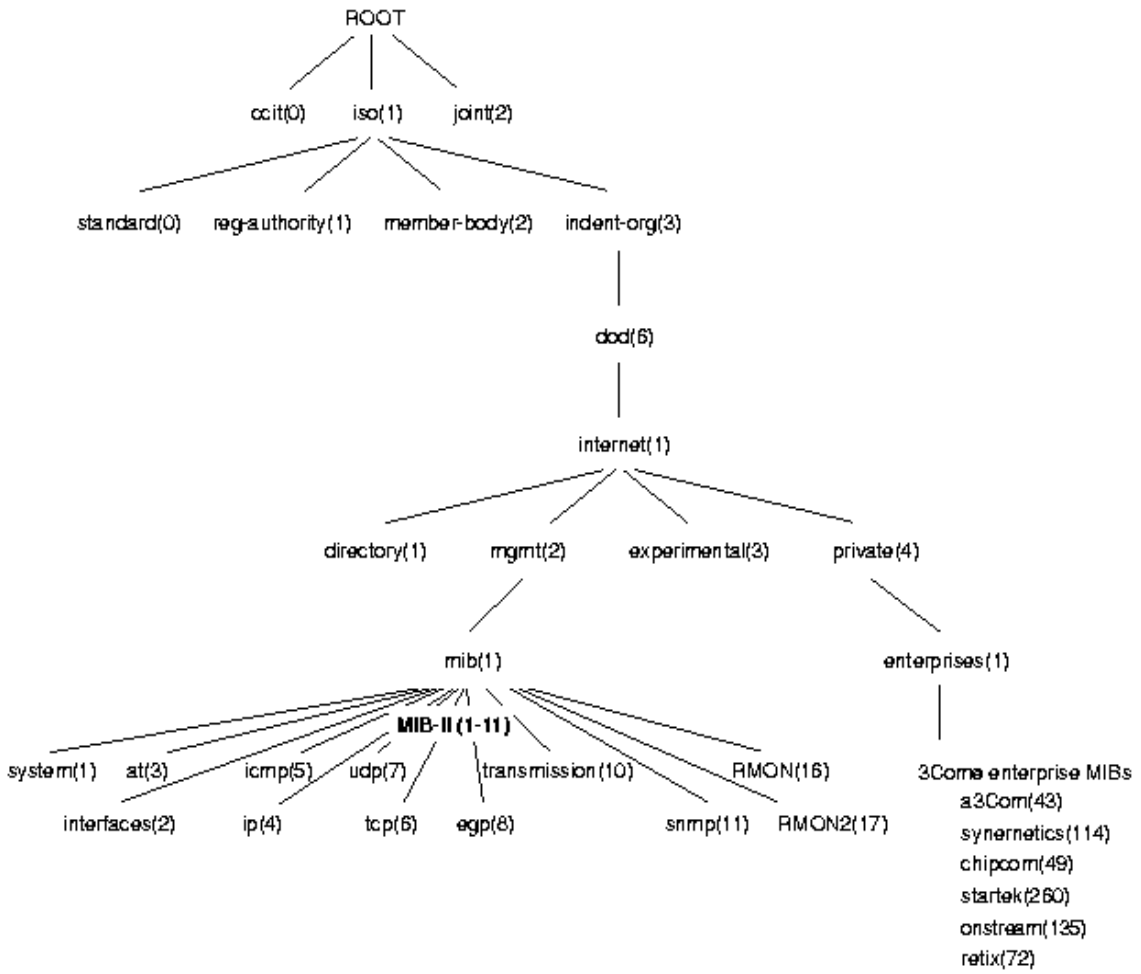


Figure 11. MIB Tree Showing Key SNMP MIBs (From: 3com)

As we can see, the MIB tree contains more general information for the network at the top and goes to more detail about devices and interfaces at the end.

Subramanian (2000, 123) refers to Abstract Syntax Notation 1 (ASN.1), which is an international standard used to name the variables in the MIB. For example, the MIB variable sysDescr in the system subtree under mib(1), describes the object.

3. Simple Network Management Protocol (SNMP)

SNMP is an application layer protocol in the TCP/IP protocol suite for accessing information in the MIB. It uses User datagram Protocol (UDP) and any network device that needs to be managed must contain an SNMP management agent. Ibe (2002, 256-259) identifies the three versions of SNMP and provides a short description:

- SNMP version 1 (SNMPv1), the first implementation, is widely used and is the de facto network-management protocol in the Internet community
- SNMP version 2 (SNMPv2) was introduced to enhance the functionality of SNMPv1 and offers a number of improvements, including additional protocol operations
- SNMP version 3 (SNMPv3) is the newest member and was designed to add security and administration features – the security shortcomings that SNMPv3 addresses are the community string which is carried as clear text as well as the permission to access partial information

4. Fixed Broadband Wireless Network Management

According to Ibe (2002, 261) there are some issues that make management of the fixed broadband wireless network different from a wired network. Wireless networks include different networking technologies and heterogeneous systems, so some special management procedures need to be considered.

The first issue includes hardware failures, like power failure and antenna and equipment failures. In addition, there is a possibility of lack of communication, even when no hardware failure has occurred. Reasons for these interruptions can be antenna misalignment or obstructions in Line of Sight (LOS) environments. The best way to avoid tuning failures is to monitor the Received Signal Strength Indicator (RSSI), so that it is above a predefined threshold. Up to now antenna alignment has been done manually and is a very difficult and demanding task, especially for fixed wireless networks covering long distances. NPS professors, Bordetsky and Bourakov, are working on the solution by placing antennas on rotators to allow their alignment to be corrected remotely from the NOC.

B. QUALITY OF SERVICE (QoS)

QoS represents the ability of the network to provide standard levels of services like performance, delivery and reliability. Ibe (2002, 265) and Sweeney (2004, 195) highlight the key parameters that are used to quantify QoS service levels:

- Latency or overall delay: the time that elapses from the instant a packet is transmitted at the source until it is received at the destination, important in voice telephony, conferencing, as well as in the TCP/IP due to the frequent acknowledgments
- Delay variation (or jitter): the variation in the arrival times at the destination of all packets belonging to the same data stream
- Throughput rate: the number of bits per second received at the destination, important in services such as high resolution video
- Availability: the proportion of time the network is operational and able to transfer users' packets
- Packet loss rate: the maximum rate at which packets can be discarded in the network, which tends to be higher in wireless networks because of the various attenuation parameters

C. NETWORK OPERATIONS CENTER (NOC)

1. NOCs for Tactical Environments

In today's Special Forces Operations (SOF) the role of operations centers is more crucial than ever. The existence of different networking platforms, applications, decision makers, and collaborative technologies improves the functionality of the tactical networks but, at the same time, increases the level of complexity in technical management as well as in interpreting information. The military control center monitors the field and the deployed forces in real-time using sensors and Unmanned Aerial Vehicles (UAVs) providing streams of information, which must be filtered, interpreted, and transformed into decision choices.

For tactical operations, NPS has been developing a conceptual model (Sense-Analyze-Adapt structure) with the desirable knowledge management architecture for wireless NOCs (W-NOCs). Figure 12 shows an iterative process which involves feedback from the sensors and decision choices (Bordetsky, 2002).

According to this model, we identify the mission and the various policies concerning the mission, answering questions related to the development and operation of network management solutions. The next step is to establish the list of functional and performance requirements and generate the set of performance metrics which allow the decision makers to measure how well the mission is executed. At the analysis stage we compare those metrics with the mission objectives and identify alternative paths of action, if needed. This Sense-Analyze-Adapt structure is a persistent feedback loop driven by the fusion of data from agents (network elements) embedded within the network and helps in the creation of a Common Operation Picture (COP) between decision makers at different levels. It is also important to note that the aforementioned iterative procedure creates an accurate situational awareness (SA) picture of the tactical network that is critical for effective management. SA is an accurate view of the critical network nodes' performance and the timeliness of the input feedback received from the network grid.

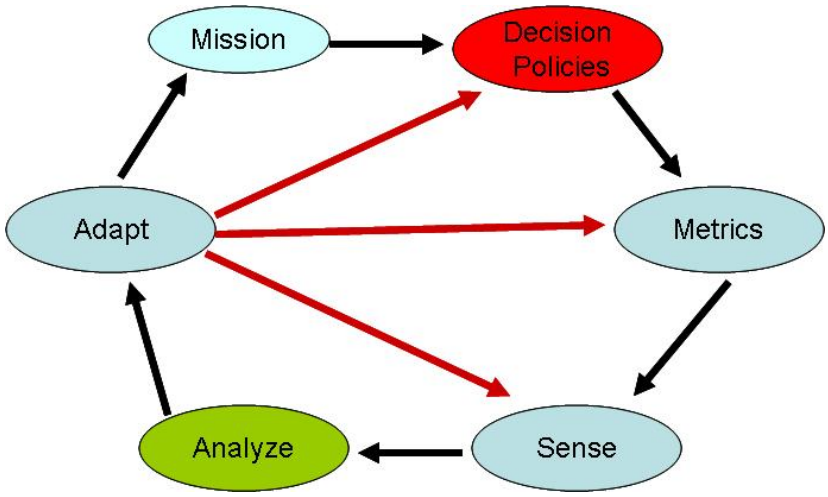


Figure 12. Conceptual Model for NOC Processes (From: Bordetsky, 2002)

As we mentioned in the first chapter, the Network Operations Center's primary goal is to constantly observe the performance of the network from a centralized location and to take corrective action, if needed, in real-time, in order to support tactical operations. It also supports the needs of operations with:

- Documentation of critical network elements and procedures

- Training personnel with the tools used to monitor network performance
- Consultation, coordination with users and general assistance in operating the network

To accomplish its mission and depending on the size of the network, three main elements are included in the NOC's structure:

a. Network Management System

This is an automated toolset of resources (software and/or hardware) necessary for detecting and troubleshooting problems, and generates various alarms and statistics from the network. Most of the NMS are SNMP-based, which means they implement the Simple Network Management Protocol and manage the network components that have an SNMP agent process integrated into them.

b. NMS Operators

These are the users at the NMS terminals who perform the configuration, monitoring, and performance functions of network management. They collect large amounts of information about network status and are trained to filter out the most significant data that the facilitator should be aware of in making a decision. They identify network problems based on events, statistics, alarms and conditions generated by the network equipment, as well as on pre-specified thresholds applied to network resources.

c. The NOC Facilitator

This is the key player who coordinates NOC management and makes all the decisions concerning the reliability and effectiveness of the network. He is the receiver of all significant inputs from the Network Management Systems and decides on the proper actions to support the tactical mission. The input that the facilitator receives from the operators is presented on screens in the NOC and can be categorized into the three levels of the network management system (NMS): performance management, configuration management, and fault management. He maintains network awareness by accepting and simultaneously providing feedback to the major elements of the network. Figure 13 shows the NOC structure and the process of creating situational awareness from NMS inputs.

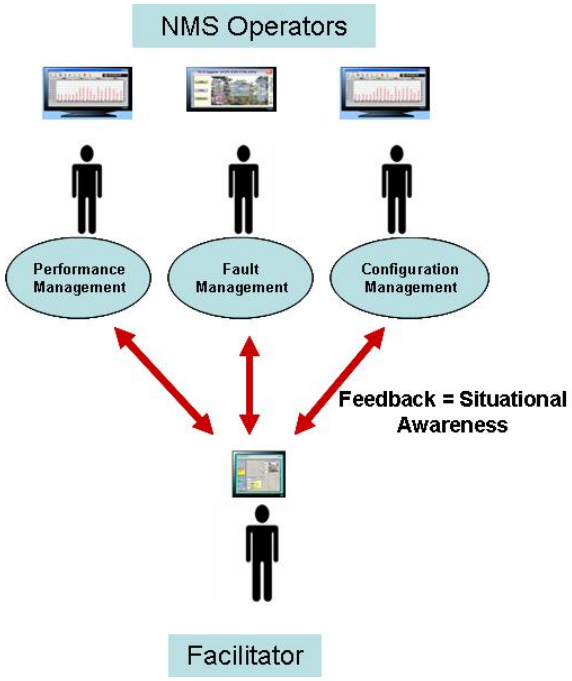


Figure 13. NOC Structure and Situational Awareness (After: 1LT Kristina S. Jeoun)

For more information on the role of the Tactical Network Operations Communication Coordinator (facilitator), refer to the bibliography in the thesis of 1LT Kristina S. Jeoun USAF, titled *The Tactical Network Operations Communication Coordinator in Mobile UAV Networks*, where this role is covered in much greater depth.

2. NPS Tactical Network Management

During TNT experiments at NPS, control over the network is distributed into different areas of responsibility and management support, which operate at different levels and cooperate with each other to provide feedback to mobile nodes and decision makers:

- CENETIX GIGA-Lab NOC for long-term data collection and management gateway to the testbed
- Deployable NOC at Camp Roberts for rapid Network Operations and feedback to air and ground Nodes
- Mobile Light Reconnaissance Vehicle for the SOF operations
- Surface Boat NOC for maritime operations

IV. NETWORK MANAGEMENT PLANNING

The main purpose of an efficient management architecture and methodology is to allow NOC operators to monitor network activities easily and to maintain the network in a proactive way by monitoring and troubleshooting alarmed conditions that may cause or indicate a degradation of services.

Every network is unique in terms of topology, software and hardware configuration, and protocol deployment. The success of managing a network depends on establishing a well organized management plan so the network operators will have the ability to allocate and extract proper information and provide analysis as well as performance predictions about network utilization.

The primary goal of establishing a network management plan is to facilitate near-term problem isolation and longer-term network planning. Network management planning is the only way to improve quality of service of mission critical applications relying on tactical network resources.

Our approach in managing the NPS tactical testbed can be broken down to the following main steps:

- Baseline the testbed
- Select appropriate management tools
- Recommend performance metrics
- Interview stakeholders to identify acceptable performance requirements for critical applications
- Model the applications' behavior using Opnet modeling tool

A. BASELINING NPS TESTBED

The main purpose of the baseline is to provide a network inventory during normal operating conditions. During baselining network operators create an overall understanding of the existing network topology and the available resources. They create

an effective history of network performance, in hopes that by understanding the past they will be able to predict the future, to a certain degree. Baselining involves recording the current state of network operation over a period of time, to serve as a basis for comparison or control (McKeller, Part I).

1. NOC Layout

The first step is to map the existing network, by creating diagrams depicting the different network levels and the main servers. It is also important to map the logical infrastructure, which documents any policies for network addressing and naming. Figure 14 illustrates the NOC subnet with the main servers and the major applications they host to perform and support network management functions and NOC operations.

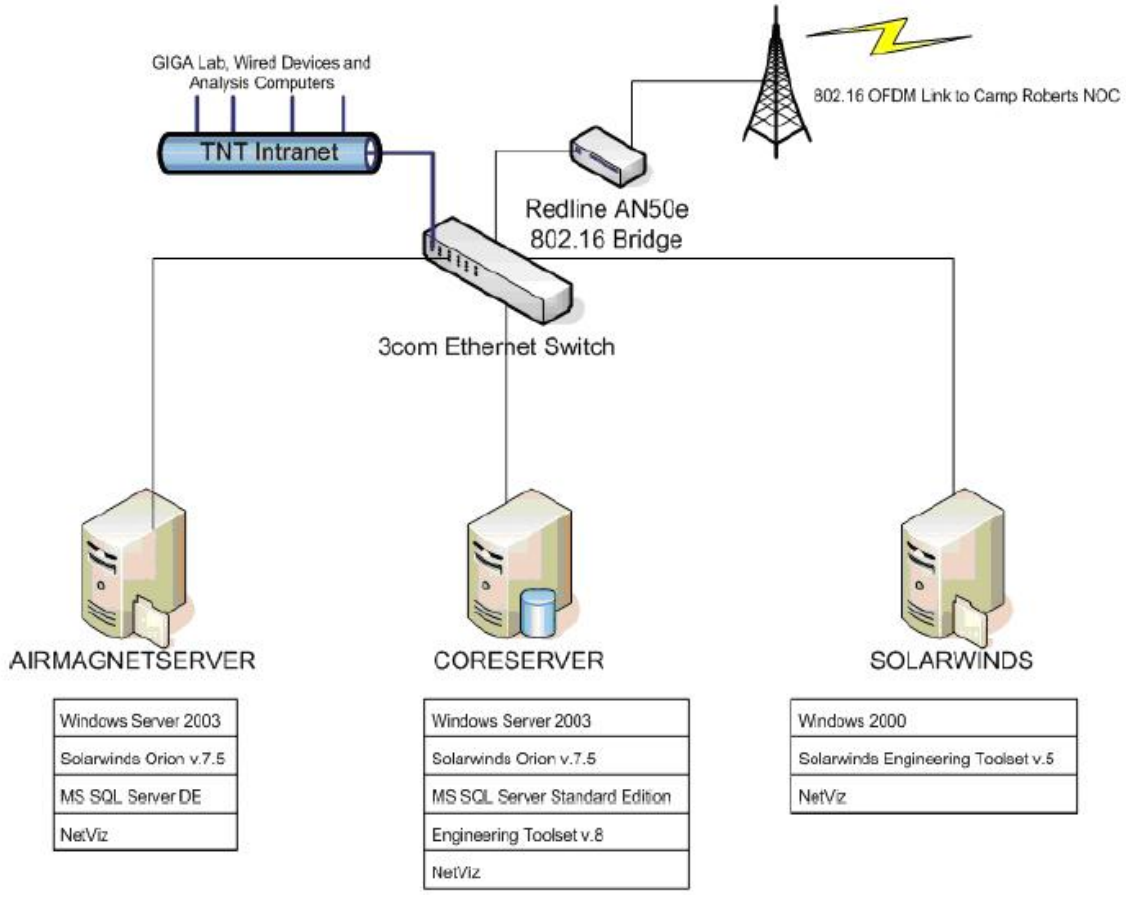


Figure 14. Schematic of NOC Layout (From: CENETIX)

2. OFDM 802.16 Backbone

The OFDM backbone segments play a critical role in providing the long-haul wireless connectivity to Camp Roberts and surface nodes in the Monterey Bay. In general the OFDM link to Camp Roberts provides high-end two-way connectivity to the sites within the backbone as well as remote access to the sensors comprising tactical air, ground, and surface mesh at Camp Roberts and Monterey Bay. Figure 15 illustrates the NPS OFDM 802.16 backbone.

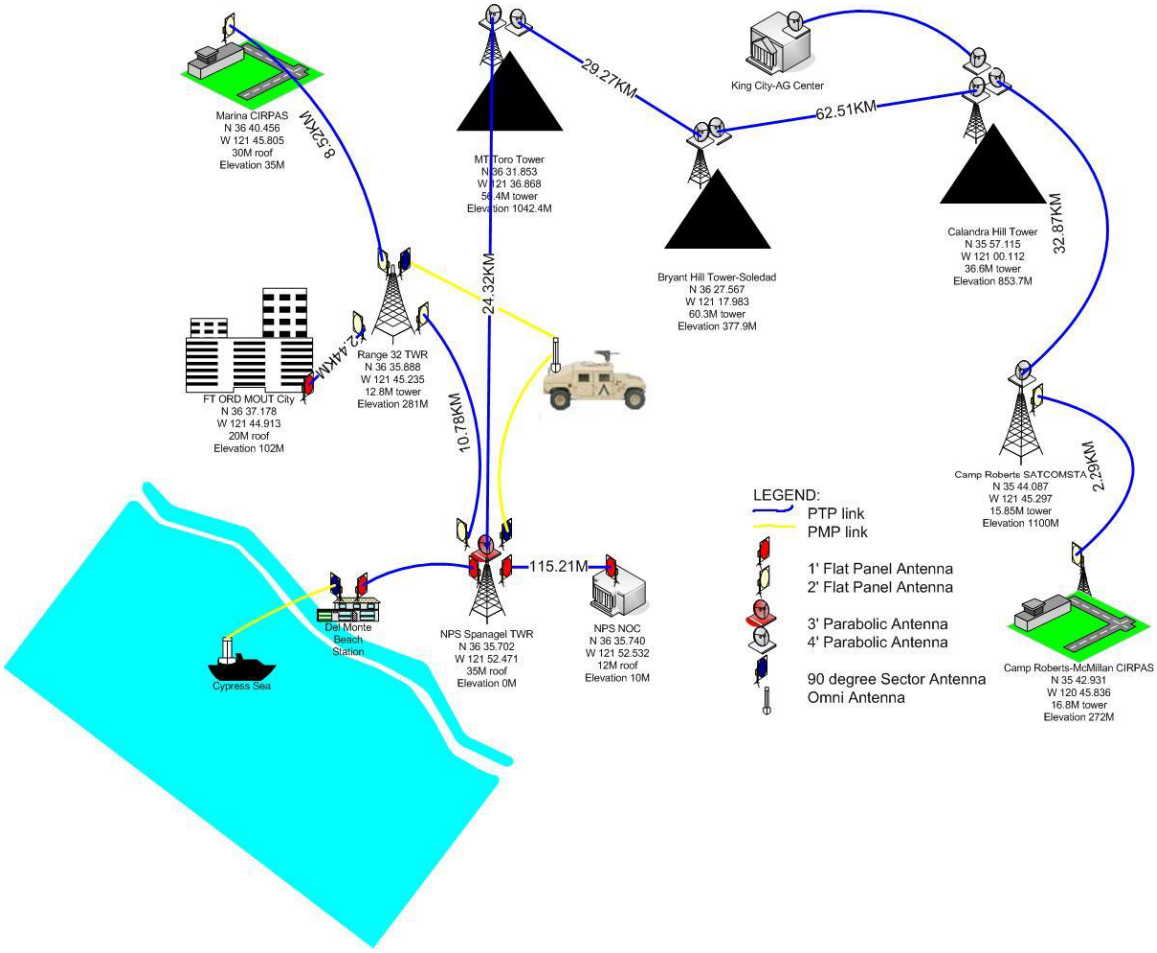


Figure 15. NPS OFDM Backbone

The TNT backbone uses the Redline Communications AN-50e 802.16 transceiver operated on a point-to-point architecture. AN-50e uses adaptive modulation of the following types: BPSK, QPSK, QAM 16, and QAM 64 data compression. The AN-50 includes an error correcting scheme which is varied along with the modulation format

and dynamically shifts between the data compression schemes maintaining the lowest bit error rate. It also provides the highest throughput when conditions over the data link change rapidly.

A web-enabled GUI is used to configure and monitor the twelve AN-50e radios of the TNT backbone. It provides general information about the configuration of the system, the received power (RSSI), the signal to noise and distortion rates, and statistics on packet transmissions on the wireless link.

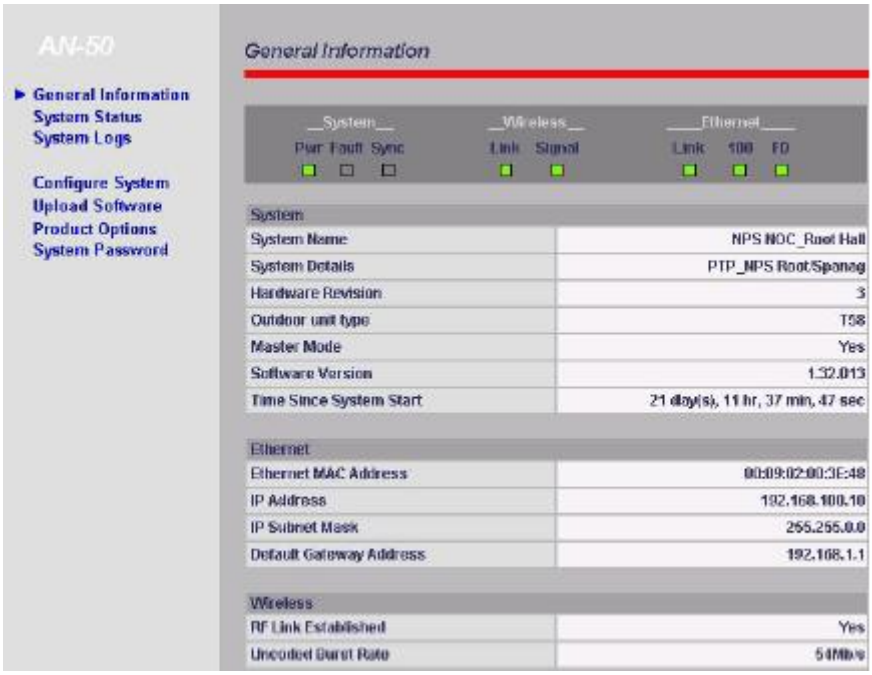


Figure 16. Redline AN-50 Web Interface

Due to the large link distances, multi-path, and RF interferences the backbone uses a maximum of QAM 16 data compression for 18 Mbps through-put. The receive sensitivity of the radio is -86dbm (received power necessary to complete a BPSK link) and losses may occur either due to the cable connecting the radio to the antenna or due to antenna misalignment.

3. Technical Objectives

The next step in network baselining is to determine the technical objectives – a number of parameters that generally define the target level of quality of service, (Oppenheimer, 2004). For the NPS testbed we can include the following parameters:

- **Scalability**, that is how much growth or expansion the network can bear. We should take under consideration the restrictions that wireless technologies impose on future expansions.
- **Availability**, the amount of time the network is operational. This parameter is expressed in percent and should be specified with great precision, because for a tactical network even 5 minutes per week (99.95%) may be unacceptable.
- **Network Performance Criteria**, these are the metrics that give us an understanding of whether or not we meet our strategic objectives. They are very helpful in identifying network degradation due to the implementation of new technologies or specific applications.
- **Security**, is one of the most important factors, but security mechanisms are sometimes implemented by the vendor's network devices due to the emerging technology.
- **Recoverability**, how easily the network can be recovered from damage or service interruption. The wireless OFDM testbed has been proven to be very reliable and stable and the cause of minor problems was identified in antenna misalignments.
- **Resiliency**, how much stress the network can handle. The major objective of NPS field experimentation is to determine maximum throughput and application performance in relation to distance.
- **Adaptability**, how agile is the tactical testbed to changes and addition of new emerging technologies.
- **Manageability**, which refers to management functions of a network: performance, fault and configuration management.
- **Usability**, how easily users of the tactical network topology can access to network resources.

4. Selection of Major Network Components for Monitoring

To be able to construct a reliable baseline for the testbed, we must define the network elements whose performance the NOC is responsible for monitoring and collect network management metrics and statistics that indicate network utilization and reliability.

a. Operation and Performance of 802.16/OFDM

A series of measurements have been done to test the reliability and quality of the 802.16 OFDM wireless long haul testbed. With the term reliability we mean QoS at the receiver. This is identified with measurements that relate to received signal strength (RSSI), Signal to noise ratio (SNR), bit error rate (BER) and available bandwidth. The throughput as a function of RSSI was investigated.

The term quality has to do with one of the most crucial measurements in the performance of the wireless backbone – the amount of packet loss when streaming multimedia. If too much data is lost, then the end user's perceived quality will be affected and may deteriorate below an acceptable level. In that case, the amount of packet loss and the received traffic should be examined.

b. NOC Servers

The servers residing at NOC perform all the network management functions, collect data for future analysis and decision making, provide software for capturing images and real-time video, and support the tactical collaborative applications. The measures of performance that should be monitored include:

- CPU utilization
- Memory utilization
- Virtual Memory usage
- Disk utilization
- Traffic in/out
- Discards and errors

A daily basis monitoring will provide potential problems and the need for upgrade or replacement.

c. Critical Experimental Network Elements

In this category fall all the network nodes that the experiment director marks as critical for the completion of the experiment and must be managed and observed. When these elements do not have compatible MIBs, packet loss and response time are the only measures of performance that we can monitor.

5. Performance Metrics (MIBs)

Some metrics are easily retrievable because they are defined as variables in the Internet Standard MIB. Other metrics are part of vendor's private enterprise MIB subtree. Finally, some metrics are not retrievable from management tools because the technology is new and the vendors have not yet implement SNMP in their equipment.

Identifying which MIBs to monitor for specific devices is a demanding task. NOC operators set thresholds and traps to specific values for determining performance requirements for network utilization and hardware operation. When that value is exceeded, an alert is generated for the NOC administrator. Monitoring MIBs and setting thresholds and alarms is a very convenient way for enabling proactive management. However, thresholds and alarms become a flood of incoming data and different kinds of measurements techniques and ways of presenting network behavior make it difficult to compare network and application performance. There needs to be a standardization of the minimal metrics we need to gather, store and present, as well as the types of information that should be available at the network operations center (NOC), thus reducing the load on the network.

Lambert (RFC 1857, 1995) highlights a set of desirable and reasonable recommended metrics (variables). Performance variables that we may use for each interface at NPS testbed:

- ifInOctets: Total number of octets received on the interface
- ifOutOctets: Total number of octets transmitted out of the interface

- ifInUcastPkts: Number of packets delivered from this sublayer to a higher layer which were not addressed to multicast or broadcast
- ifOutUcastPkts: Total number of packets that higher level protocols requested be transmitted and which were not addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent
- ifInNUcastPkts: Number of packets delivered from this sublayer to a higher layer which were addressed to multicast or broadcast address at this sub layer
- ifOutNUcastPkts: Total number of packets that higher level protocols requested be transmitted and which were addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent
- ifInDiscards: Number of inbound packets which were chosen to be discarded, even though no errors had been detected to prevent their being deliverable to a higher layer protocol – one possible reason is to free up buffer space
- ifOutDiscards: Number of outbound packets which were chosen to be discarded, even though no errors had been detected to prevent their being transmitted – one possible reason is to free up buffer space

Performance variables that we may use for each network node:

- sysUptime: Time since the NW management portion of the system was last re-initialized
- ipForwDatagrams: Number of input datagrams for which this entity was not the final IP destination – as a result an attempt was made to find a route to forward them to the final destination

- ipInDiscards: Number of input datagrams for which no problem were encountered to prevent their continued processing but which were discarded (for lack of buffer space)

During our research, we came across a set of performance variables from various sources. An extensive list of these performance variables and their analytical description is presented in the Appendix.

6. Centralized Network Management Software Selection

The main purpose of the NPS NOC team is to perform network management, oversee network performance, and capture specific data about TNT nodes' performance. The ongoing network monitoring at NPS testbed is necessary to ensure network optimization and application performance, because different wireless technologies are tested quarterly. Having a baseline and knowing network behavior and traffic shaping under certain conditions, we can take action to control the performance of traffic flows based on experimental priorities. Management software that polls the monitoring devices over the network and collects statistics on certain performance metrics is the critical element at the NOC's disposal. The collected information from each network node is maintained within a central database which is valuable for identifying trends as well as determining traffic patterns. The data can be viewed in various intervals such as days, weeks or months.

There are numerous commercially available NMS such as Hewlett Packard's Open View, Cabletron's Spectrum, Tivoli, Sun Solstice, Intel LANDesk, and Netscout Webcast to name a few. Subramanian (2000, p485) classifies them as low-end NMS, enterprise management solutions, and enterprise NMS.

Low-end NMS are usually PC-based or NMS for vendor specific network products. Tivoli is an example of an enterprise management solution for demanding network environments that can handle up to 10,000 network nodes.

Enterprise NMS is the most widespread solution with HP Open View and Spectrum being the most popular. Their platform architecture is open modular and distributed and provides interfaces for other third-party NMS to filter information and send it to a centralized management station for an aggregated view.

The tools that have been chosen by the NOC to perform network management and data collection are Solar Winds Orion and Solar Winds Engineering Edition. CENETIX has a license for them and they are the most suitable for the testbed because they are simple, provide an easy to use interface, and don't generate unnecessary traffic.

a. Solar Winds Orion

The Orion Network Performance Monitor (NPM) is a comprehensive, web-based, fault management and availability and bandwidth performance management application that enables the NPS NOC to view real-time statistics and availability of the network directly from a custom web browser. The main functions of Orion NPM are Network Discovery, Map Maker, Web Interface, Nodes View, and Systems Management.

Using Orion Network Performance Monitor, the NOC operators are able to monitor and collect data from switches, servers, and any other SNMP enabled devices. For devices without SNMP enabled, such as the Redline AN50e bridge devices that connect the OFDM link, only response time and packet loss can currently be monitored. Additionally, Solar Winds Orion is used to monitor CPU Load, Memory utilization, and available Disk Space on select devices that support RFC 1213 compliant MIB. SQL Server 2000 was also installed on the same box as Orion to increase the data collection ability and simplify the NOC operations and data retrieval.

b. Solar Winds Engineering Toolset

The Solar Winds Engineering Toolset is used by the NOC operators, in addition to Orion, primarily for network discovery and monitoring. It is a real-time network monitor that can track network latency, packet loss, traffic and bandwidth usage, and many other network statistics, and is also capable of graphing data from MIBs of interest.

c. Other Resources and Tools

In addition to the aforementioned network management systems, there are some other tools that help network operators to monitor and present the performance of network elements.

- **OpManager** is a powerful NMS with the same characteristics as Solar Winds and is being used for the last two experiments as a supplementary

NMS. The version 5.1.5 which is installed has the ability to monitor only ten network devices or applications. The network operator can configure different views, alarms or create custom reports.

- **RF link monitoring tool** is a small utility provided from Redline that enables the network operator to see the status of the backbone links. The value of the Received Signal Strength Indicator (RSSI) can point to problems due to antenna polarization, 1st Fresnel Zone obstructions and weather conditions.

- **Microsoft Producer** is being used to capture screenshots by the NOC Operator. These screenshots contain throughput visualizations and average response time graphs of network performance on various nodes used in specific tactical scenarios.

7. Typical Applications in Tactical Testbed

Another important factor is to identify the typical applications that generate the observed traffic loads. The NPS tactical testbed uses two software tools to facilitate the virtual collaborative environment, providing a network-centric view of the mission area and fulfilling the needs for information sharing and establishing situational awareness.

The primary tool for collaboration is “Groove Virtual Office”, a client application that functions as a peer-to-peer collaborative tool and provides any user that is connected by a network the ability to participate in a common, self-synchronizing work space for file sharing. It also provides real-time text chat and streaming video connectivity. Data that are posted by any participant in Groove will be automatically shared with all other online nodes in the same workspace. Groove can be used offline utilizing the coordination of a relay server that synchronizes all systems assigned to a workspace. In case the network is down, data will be automatically synchronized when connectivity becomes available again.

The second tool being used during TNT experiments is the “SA multi-agent system.” SA is a client-server application that has been developed by CENETIX faculty, to provide a common operating picture (COP) to the participants in experiments and increased situational awareness to the war fighters and network operations centers. Real-

time data are represented by various icons in a two dimensional map of the operating area. All events are relayed from the agents to the server located at NPS NOC and the server synchronizes the data with all the agents to provide a COP.

For a tactical network a major concern is to increase the throughput for mission critical applications. According to Oppenheimer (2004, p41) factors that constrain application layer throughput include the following:

- End-to-end error rates
- Protocol functions, such as handshaking and acknowledgments
- Frame size
- Lost packets at internetworking devices
- Performance of Workstations and servers: Disk-access speed, Device driver performance, CPU and memory performance, application inefficiencies or bugs, operating system inefficiencies

8. Traffic Analysis

The next step in baselining the tactical testbed is to collect samples of network traffic, analyze them, and finally, obtain the network activity profile. The sampling periods must include times where the traffic loads reach a peak. The NPS tactical testbed is used primarily in quarterly field experiments and it is not connected to the campus network, so we don't have traffic due to Internet users or client-server applications.

We can distinguish two cycles of operation: the normal and the experimental. During the normal cycle we have no activities in the network and it is sufficient to monitor the average utilization levels on the wireless OFDM 802.16 backbone network (fault management). The experimental cycle of network operation lasts about two weeks each quarter. Since the testbed is used mostly in experiments, the baseline depends on specific applications and experiments with new technologies. Based on the collected data we identify the hosts, applications and users who are responsible for network activity, and we determine whether the error levels for each critical network node are kept within acceptable limits.

B. TNT 05-4 FIELD TRIAL AND SUPPORTING MANAGEMENT FUNCTIONS BY THE NPS NOC

TNT 05-4 presented a great opportunity to establish a baseline for the tactical testbed as well as to identify the supporting operations by the main NOC (NPS) during the field experiments. The Main NOC successfully participated in and supported the Above and Below Water SA for Combat Swimmer, Connectivity and Collaboration for Radiation Awareness, Biometrics Fusion, Maritime Interdiction Operations, and experiments involving the Light Reconnaissance Vehicle (LRV). The main purposes of the NPS NOC for TNT 05-4 were to perform network management, oversee network performance, and capture specific data about TNT nodes' performance.

The polling interval was set at 10 seconds for every interface and specific thresholds for network nodes were defined in Solar Winds Orion to generate alarms for proactive management. The network manager was informed when utilization of certain devices and applications had reached the specified limit through the use of network alarms and thresholds. Additionally, Orion was used to monitor CPU Load, memory utilization, and available disk space on critical nodes and servers at the main NOC, which support RFC 1213 compliant MIB.

1. 802.16 OFDM Backbone Performance

Using Solar Winds Orion's Web Interface, the NOC facilitator was able to view the fixed 802.16 backbone in real-time. Figure 17 shows the model of the OFDM link architecture and the status of the Redline AN-50 backbone nodes with green color. In case there was a problem, the color turned to yellow or red, providing timely network awareness to the NOC operators. In addition, Orion provided the ability to "drill down" to a view of the nodes at remote subnets, like Real Lab and Camp Roberts.

The RF link monitoring tool (Figure 18) enabled the network operator to see the value of the Received Signal Strength Indicator (RSSI) in real-time, as well as the value of the Signal to Noise ratio, which suggests the existence of RF interference.

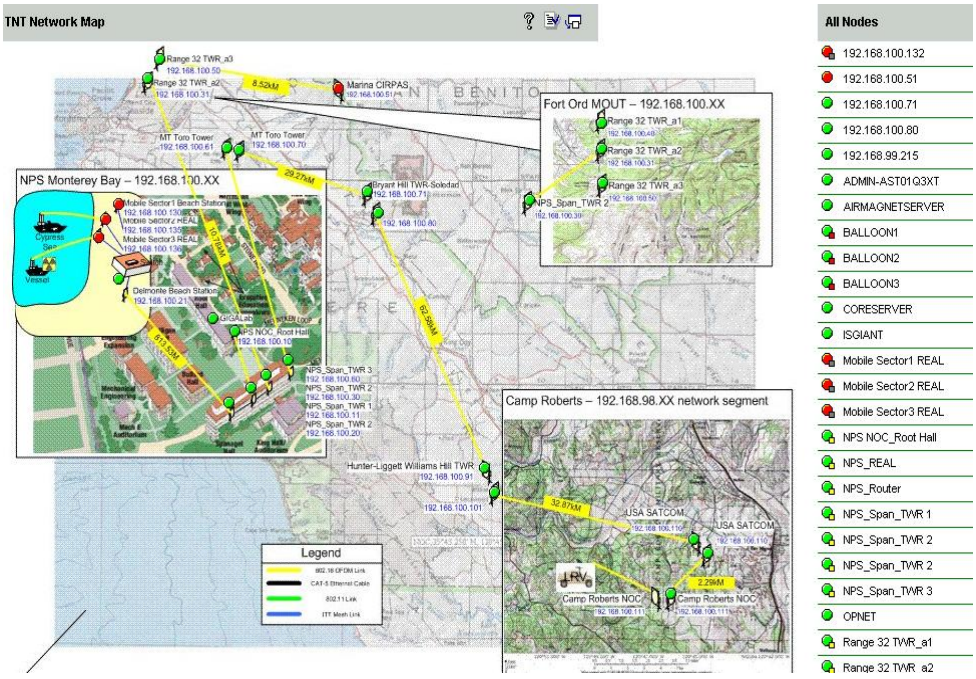


Figure 17. Real-time View OFDM Backbone

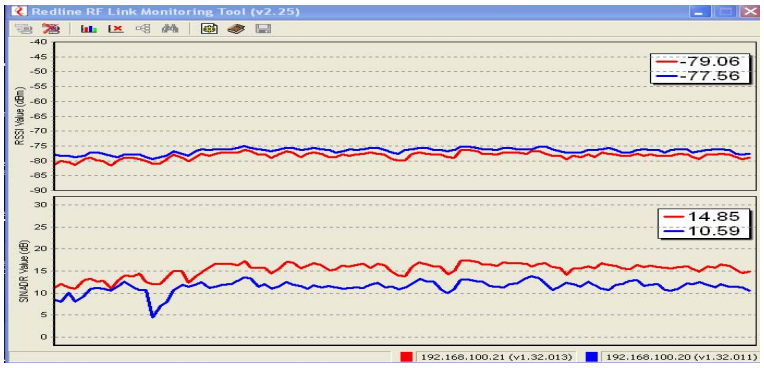


Figure 18. RF Link Monitoring Tool

2. Tactical Extension of 802.16 OFDM to the Sea - Collaboration for Radiation Awareness, Biometrics Fusion, and Maritime Interdiction Operations

The experiment was conducted with the objective to test the use of broadband backhaul, capable of transmitting mission critical data through ships superstructures and cargo containers efficiently and effectively for future maritime and port security interdiction operations. Boarding team assets included video capture devices allowing biometrics fusion, cargo tracking, audio communications, portable radiation detection

unit data, and digital document acquisition and transfer. A tactical OFDM 802.16 extension was established connecting all networking assets and the NPS NOC for providing situational awareness, a common operational picture, and collaborative behavior.

Technologies that were evaluated during the maritime experiment were: The Man-Pack 802.16 OFDM backhaul link, LLNL Ultra-Wideband (UWB) interface and portable biometrics gathering equipment.

Solar Winds IP Network Browser was used to scan the subnet and capture a real-time picture of which nodes were in the network. Then those devices were added into the Network Monitor for real-time monitoring of their status. Figure 19 shows the daily Network Monitor view, displaying all the OFDM backbone nodes and the critical nodes as well. The NOC facilitator was able to keep track of the response time and packet loss and take necessary actions to maintain connectivity in case of a generated alarm.

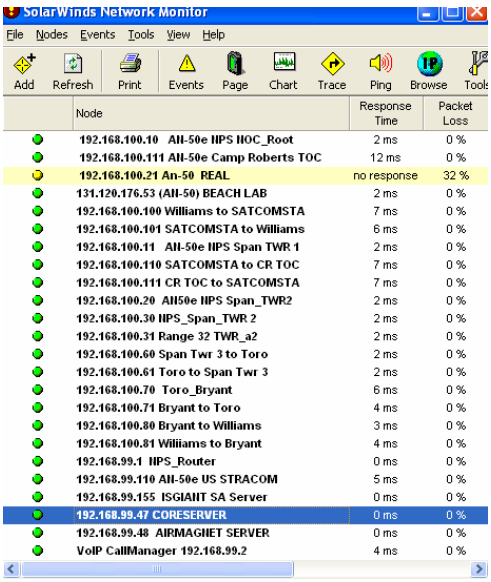


Figure 19. Network Monitor: Daily View

The experiment started with testing video transmission from the boarding officer through the Groove collaboration tool at 0940. Figure 20 illustrates the alarms when there was a packet loss above 10%. At the same time the latency of the backbone link was

monitored. From Figure 21 we can see that during the usage of Groove for video and file transfer, the response time is increased from 5.5 ms to 13 ms.

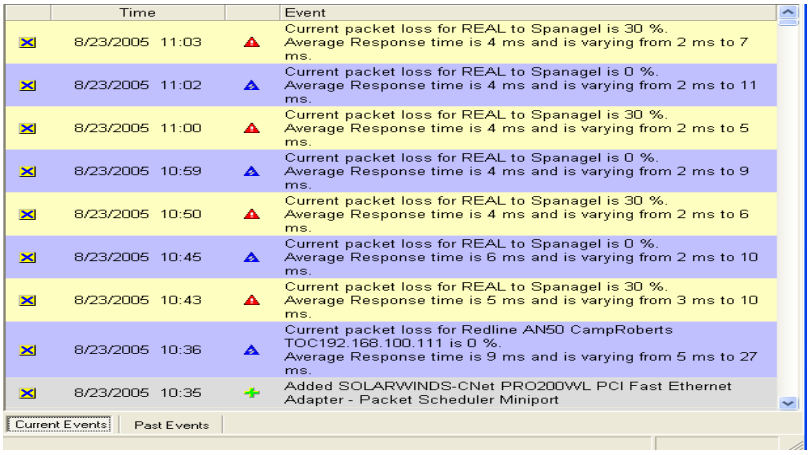


Figure 20. Alarms and Thresholds

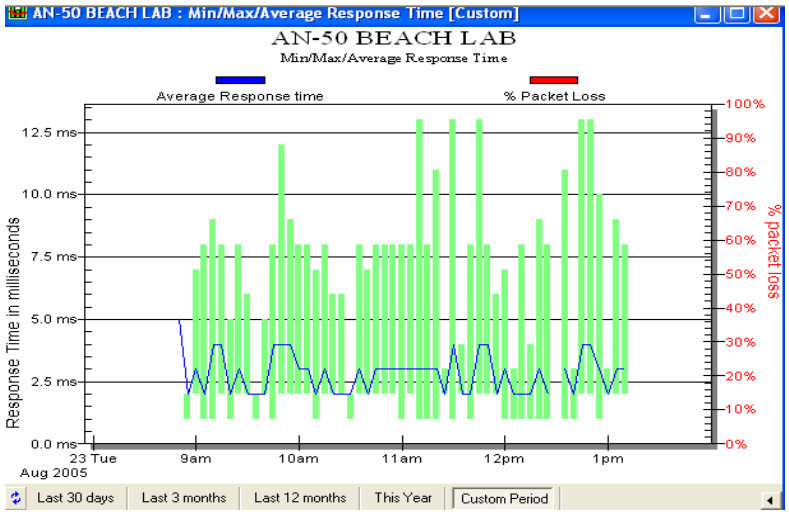


Figure 21. Backbone Latency

The network manager was informed when utilization of certain devices and applications had reached the specified limit through the use of network alarms and thresholds. Alarms were generated for the Solar Winds server when disk utilization was above the specified threshold (70%).

Groove software was used as the collaborative tool between the boarding officer, NPS NOC and LLNL. The boarding officer, using the same Groove workspace, uploaded

biometric & radiation files for analysis. Figure 22 illustrates the throughput as well as the traffic (transmitted-received) during the experiment. The spike indicates the file transfer.

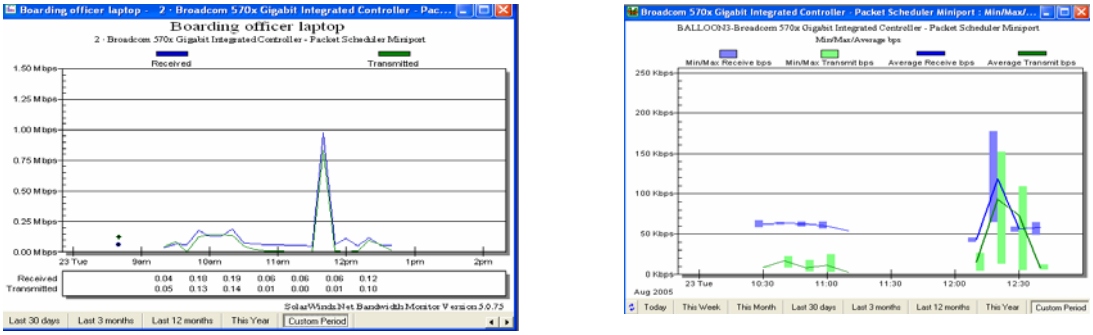


Figure 22. Traffic during Groove

Around both 11:30 and 12:40, we observe the highest latency in network performance, which was due to file and video transfer. The quality of transmitted video during shipboarding was excellent. As it can be seen from the data analysis, the OFDM link reliability and the common operation picture using collaborative technologies were a success, despite the heavy traffic generated.

3. Light Reconnaissance Vehicle (LRV)

The Light Reconnaissance Vehicle (LRV) prototype is a ground mobile platform that can maintain effective situational awareness in remote locations and provide local and long-haul data and voice communications to support dismounted tactical forces in the field. TNT 05-4 experiments incorporated some innovative wireless and collaborative technologies into the LRV to determine tactical suitability in providing command, control and communications to the “last tactical mile” as a network-centric transformative effort. The LRV acted as a bridge between the SOF LAN and the TNT OFDM backbone. The ITT Mesh was the primary wireless communications protocol during the high value target (HVT) search mission scenario, enabling SOF team to transmit real-time video, voice and data traffic.

Using the Solar Winds real-time tools, the NOC was able to monitor the performance of critical nodes, at any given time, according to the following parameters:

- Influence of terrain profiles and required range for maximum throughput
- Video Quality

- Integration of Situational Awareness functions
- Evaluation of link performance, while simultaneously collecting data from different network nodes
- Network stability during experiments

The network monitor provided the visibility to the NOC facilitator to track the current status (up or down) of critical nodes (Figure 23). This function was proved to be extremely useful in SOF mesh topology due to the constant movement. The main NOC was able to see the status of the link and tell the LRV commander to take corrective actions, in case there was no connectivity.

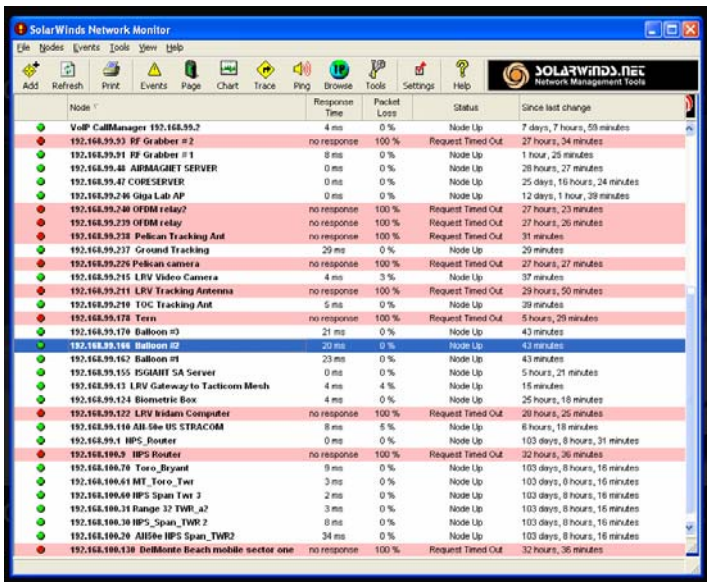


Figure 23. Real-Time Monitor of Network Status

The handheld Tacticomp devices provided by Inter4 Corporation were used in the wireless mesh network topology, providing video, voice and data into the TNT testbed. The main NOC using real-time graphs and management tools was monitoring the performance of the critical nodes. From Figure 24 below, we can see performance characteristics while LOS was maintained between the mesh nodes and they were within proximity of the LRV. Average response time for the Gateway to the mesh network was 8 ms and at approximately 13:40, a packet loss of 20% was observed, due to the distance between the mesh nodes.

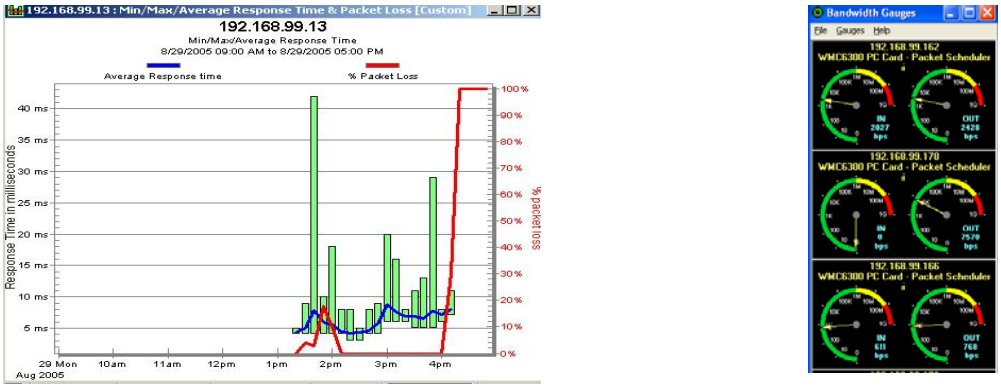


Figure 24. Mesh Gateway Performance and Performance Gauges

Real-time video and voice communications contributed to the enhanced situational awareness and common operation picture. Figure 25 illustrates the situational awareness in the SA application, when motion was detected from the sensor (Smart Rock). SA provides a visual representation of the response time, throughput, and packet loss from the agent. The Ruler, which is a function of the SA, allows users to make quick measurements of distance between nodes on the screen.

Figure 25. Real-Time Video and Motion Detection from Sensor

During the experiment a wireless link was established between a surrogate UAV (Pelican) and a tracking antenna on the LRV. Figures 26 and 27 show the performance graphs from data collected by the NPS NOC regarding the LRV video camera and the tracking antenna.

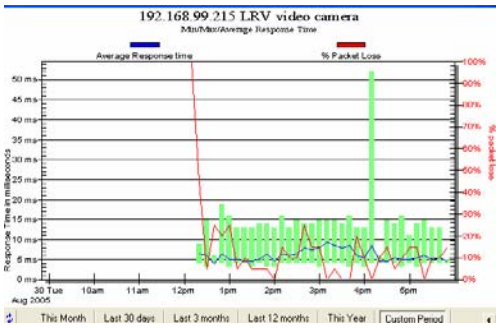


Figure 26. LRV Camera Response Time

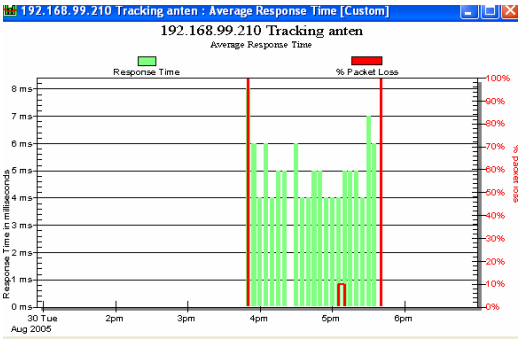
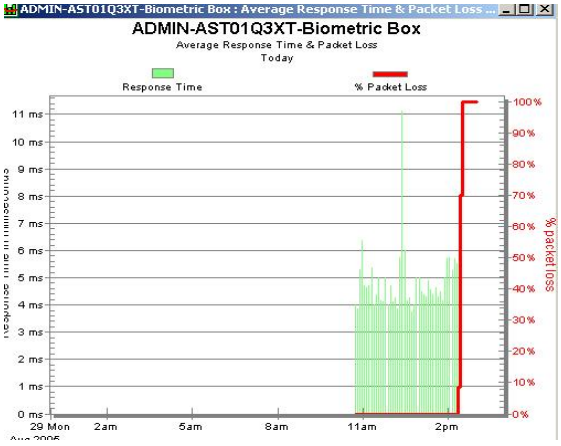


Figure 27. Tracking Antenna

Biometrics data was also transferred across the ITT Mesh and TNT network and through a VPN connection to National Biometrics Fusion Center (NBFC). Transfer of the fingerprint file to NBFC using this method took less than 10 seconds with a verification response within 10 minutes. Performance graphs in Figure 28 illustrate a higher response time (spike) during the transmission of the biometrics files, shown with the green.



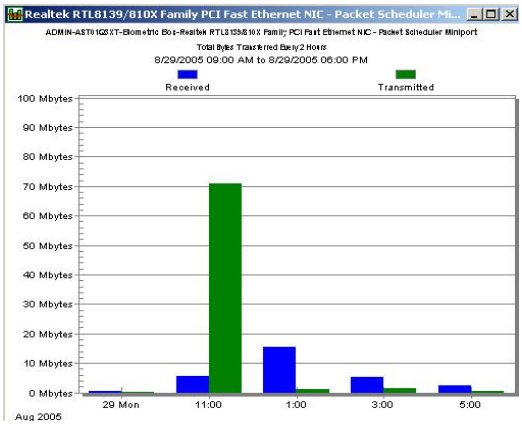


Figure 28. Biometrics Response Time and Total Bytes

NPS NOC personnel determined thresholds to monitor the performance of the main network servers at CENETIX. The polling interval was set at 10 seconds and the thresholds for generating alarms at 80% for CPU load and 75% for memory utilization. From the histogram in Figure 29, we can see degradation (yellow alarm) for the CPU utilization of the server with the network management software, and the amount of the

received traffic that exceeded the specified threshold. This happened because at the same time the server was accepting SNMP messages from polling all the network nodes, video from Groove was running and the NOC officer was using software for data capturing.

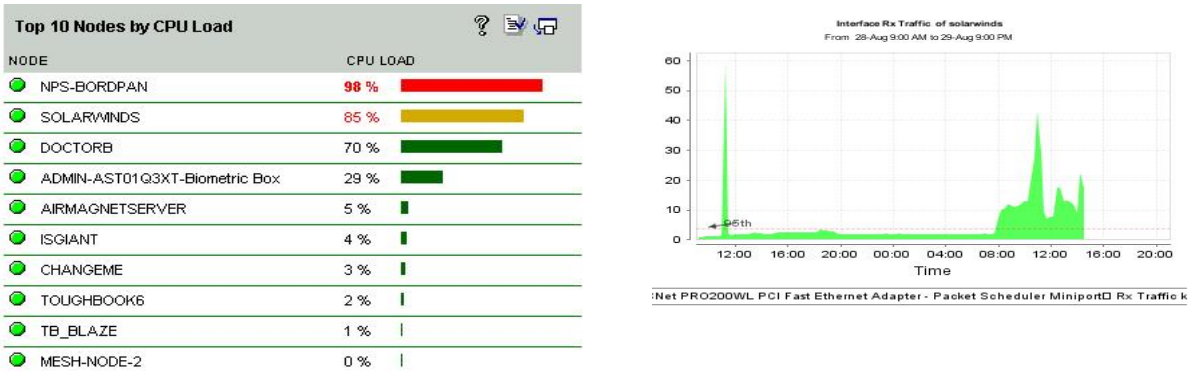


Figure 29. Yellow Alarm for CPU Load and Traffic Load on the Server

C. CONCLUSIONS

1. OFDM Backbone

Response time - No user, especially in tactical networks, would like to have large response time in network behavior. Users are able to realize the delay when response time is beyond a certain limit. For protocols that offer reliable transport and interactive applications the 100 ms threshold is often used as a timer value (Oppenheimer, 2004).

The OFDM testbed performed remarkably well for providing the long-haul wireless connectivity to Camp Roberts and surface nodes in the Monterey Bay. Figures 30 and 31 illustrate stable patterns for both NPS-Camp Roberts link and NPS-Beach Lab link, observed at the IP (layer 3) level of OFDM backbone performance. The maximum response time for the AN-50 at the NPS NOC had reached 80 ms while at the same time the maximum response time for the AN-50 at Camp Roberts was 250 ms. Average response time during operations was around 5-6 ms.

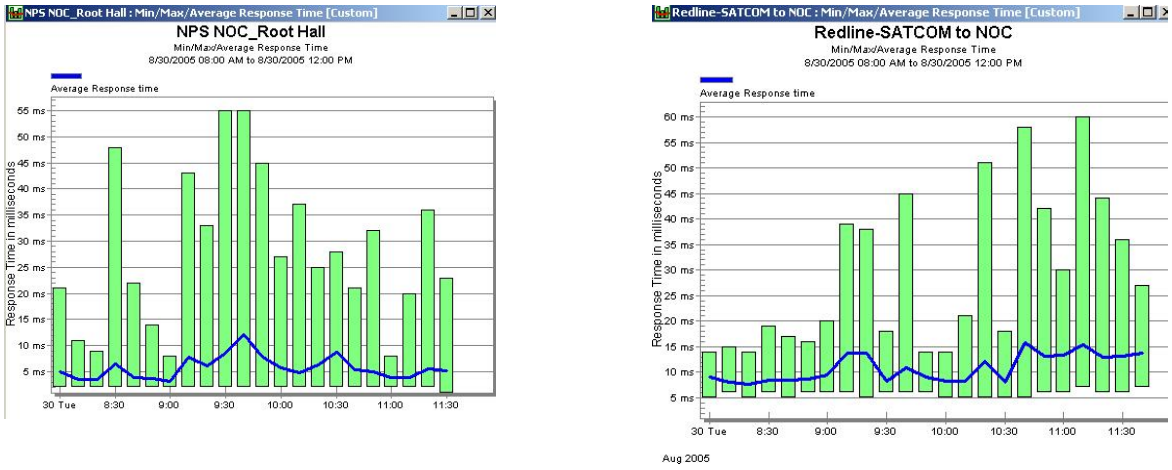


Figure 30. NPS-Camp Roberts Link

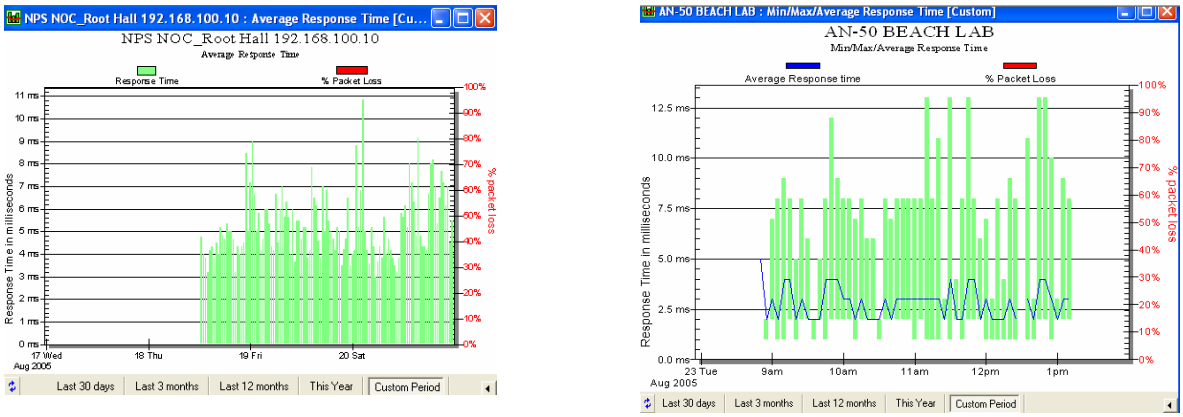


Figure 31. NPS-Beach Lab Link

Network utilization - The optimum average network utilization for wide-area networks is up to a level around 70 percent (Oppenheimer 2004). At this level of utilization, peaks in network traffic can be handled without obvious performance degradation. 802.16 OFDM provided two-way connectivity without any congestion, to the sites within the backbone as well as remote access to the sensors comprising tactical air, ground, and surface mesh at Camp Roberts and Monterey Bay

Testbed accuracy – Accuracy can be achieved when the data sent by the source are the same at the destination and the bit error rate (BER) threshold specifies the acceptable level of performance. We can approximate a BER by comparing the number of errors to the total number of bits. Oppenheimer (2004, p. 42) states that a good threshold to use is that there should not be more than one bad frame per 10^6 bits. Figure

32 illustrates stable behavior of the OFDM NPS-Camp Roberts backbone with rare moments of small percentage packet loss contributed to antenna alignments.

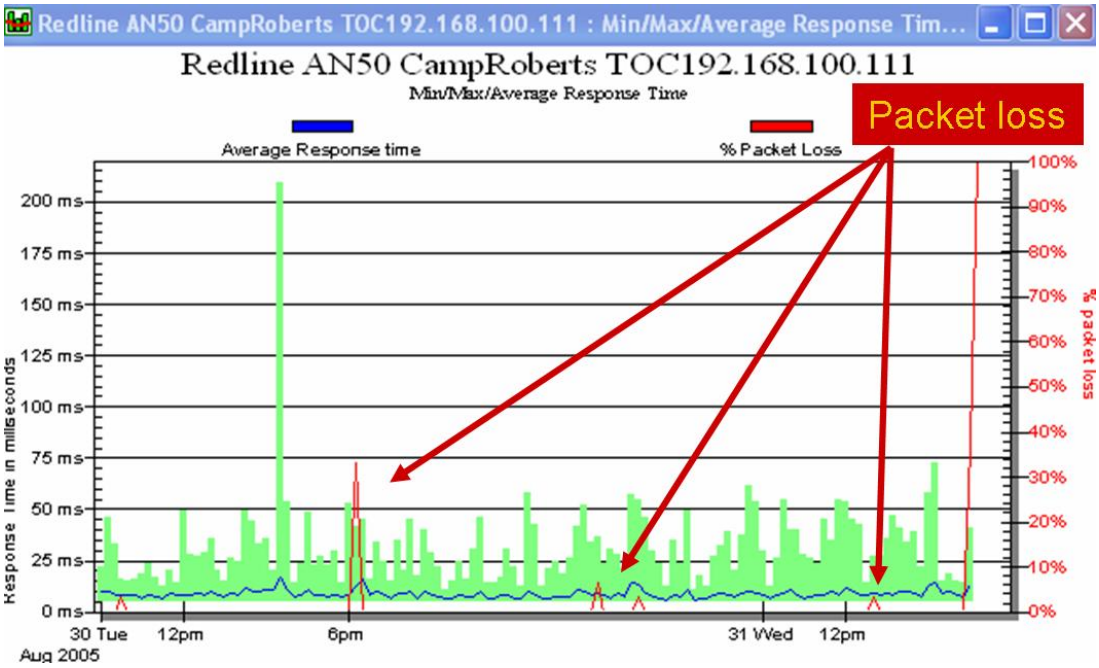


Figure 32. Camp Roberts AN-50 Packet Loss

Delay (jitter) - The major goal of tactical networks is to provide constant feedback and situational awareness to the end-users: war fighters. This is the reason that a minimal delay is required for mission critical applications. Moreover delay must be constant for voice and video applications.

Ethereal (www.ethereal.com), is a very useful, freely available packet analyzer, which helped us to analyze and inspect packets from video applications, during our research. The graph in Figure 33 represents the sequence stream for video application as a straight line, confirming the quality of video transmissions on the OFDM testbed.

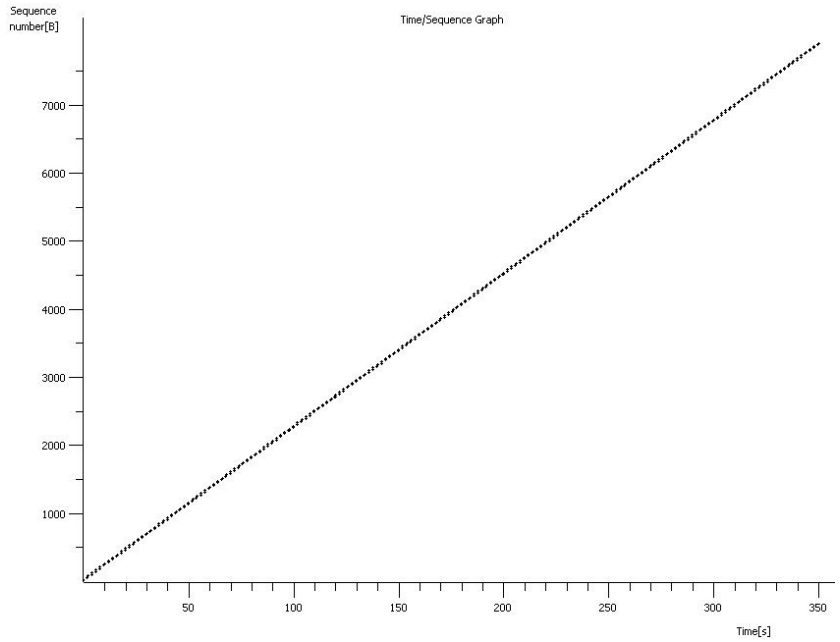


Figure 33. Sequence Stream for Video Application

Received Signal Level – One of the most important factors for the wireless OFDM backbone is the RSSI. According to the manufacturer's specification, the Redline AN-50 provides for received signal sensitivity about –86 dB and a minimum throughput of 6 Mbps. This is the lowest received power necessary to complete a BPSK link. To achieve higher order modulations and higher throughput, larger received signal strength is required. The following table summarizes the various modulation types and data rates that are used in the AN-50 radios.

Modulation	Coding Rate	Over The Air Rate (Mbps)	Uncoded Burst Rate (Mbps)	Average Ethernet Rate (Mbps)
BPSK	½	12	6	5.82
BPSK	¾	12	9	8.63
QPSK	½	24	12	11.38
QPSK	¾	24	18	16.7
16 QAM	½	48	24	21.77
16 QAM	¾	48	36	33.01
64 QAM	⅔	72	48	44.1
64 QAM	¾	72	54	48.8

Table 3. AN-50 Modulation Schemes and Throughput (From: Redline)

The variation of the RSSI value was investigated with several tests in basic backbone nodes. Since the Redline's MIB was not compliant to the Solar Winds', a CENETIX in-house developed application in Visual Basic was used, to collect the RSSI values from four AN-50 radios in eighteen-hour time intervals. The raw data was entered into Excel for data analysis and the performance from the backbone is shown in the following table:

IP	NAME	Median RSSI	Max RSSI	Min RSSI
192.168.100.10	NPS NOC	-60.31	-58.81	-66.31
192.168.100.11	NPS Spanangel Tower	-36.88	-35.56	-44
192.168.100.110	CR-SATCOM	-71.38	-69.31	-74.56
192.168.100.111	CR-CIRPAS	-79.94	-73.81	-77.56

Table 4. RSSI for Main Backbone Nodes

Figure 34 illustrates an unstable behavior of the OFDM NPS-REAL backbone, due to NLOS conditions and maybe antenna misalignment, observed at the wireless (layer 2) level with RF link monitoring tool.

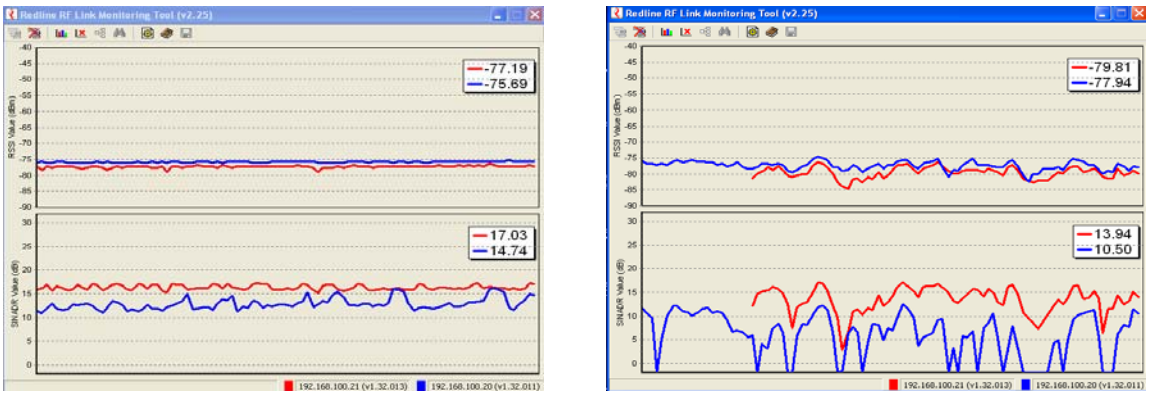


Figure 34. Normal RSSI and Irregularities for the REAL AN-50

Efficiency – The last performance goal was to gain an understanding of the efficiency of collaborative applications running on the tactical testbed and determine if

these applications and protocols use the available bandwidth effectively as well as how much overhead is required to send traffic. A very powerful tool, OPNET Modeler Application Characterization Environment (ACE) was used to model network behavior and associate application and network performance patterns in a holistic network behavior model. OPNET capabilities and the results from modeling the TNT testbed are presented in a later chapter.

2. Role and Responsibilities of the NOC

The NOC's major responsibility is to manage the testbed and perform all the necessary actions to prevent downtime. In addition, because of the ad hoc nature of the tactical last mile operations, the NOC should be capable of facilitating the communication channels inside the management grid, providing the right information at the right time.

During TNT 05-4 field experimentation, several Network Operation Centers were deployed, capable of working in harmony over the OFDM backbone: the main NPS GIGA Lab NOC, the Deployable NOC at Camp Roberts, the mobile ground NOC in the LRV, and the mobile surface NOC in the Cypress Sea boat. In this distributed architecture the NPS NOC became the remote center for long-term network performance, configuration, and fault monitoring data collection. The NOC also supported the integration and deployment of different wireless platforms for improving tactical mission performance capabilities and achieving reasonable situational awareness of network actions and behaviors. An automated approach was used to capture network node data, and store them in a standardized SQL compliant database for easy retrieval and post-exercise analysis.

The real-time visual model of the OFDM backbone, using ORION web interface, increased the situational awareness of the NOC facilitator and helped him to identify problems with the reach back capability of the OFDM link both to the TOC at Camp Roberts and the surface NOC, and to visually determine node status of wired and wireless mesh systems during experimentation.

Data collection for that experiment also contained screen shots of throughput visualizations and average response time graphs of network performance on various nodes used in the tactical scenario.

Below is a table which identifies network operation functions and the tools used for each management area.

Management Area	Vendor Specific Area	Tool Used
Configuration Mgt	Discover (Solar Winds)	• IP Network Browser • Ping Source
Performance Mgt	• Performance Mgt (Solar Winds) • Solar Winds Orion	• Network Performance (Monitoring : min/max/avg bps in/out, Total bytes transferred, avg response time) • SNMP Graph (MIBs of interest) • Bandwidth Gauge (in/out bps)
Fault Mgt	• Monitoring (Solar Winds) • RF Link Monitor (Redline)	• Network Monitor : (Fault indication, Response time, Packet loss, Node status) • Monitor Link RF Status • RSSI (dBm) • SINADR (dB) • Monitored two ends, 192.168.100.10/NPS NOC and 192.168.100.111/Camp Roberts TOC
Situational Awareness	SA Agent	Used to monitor alarms, motion and node status

Table 5. Network Operation Functions Administered by the NOC

THIS PAGE INTENTIONALLY LEFT BLANK

V. TNT 06-1 RAPIDLY DEPLOYABLE NETWORK CONCEPT OF OPERATIONS

Having overcome technical challenges in innovative wireless technologies, the next cooperative field experimentation (TNT 06-1), between the United States Special Operations Command (USSOCOM) and the Naval Postgraduate School (NPS) was conducted in Camp Roberts, CA from 14-18 November 2005 and in Alameda, CA from 20-22 November. The overall objective of TNT 06-1 was to investigate the applicability of advanced communication technologies in support of both Special Operation Forces (SOF) missions and net-centric warfare.

More specifically, the objective of this experiment was to test and evaluate the ability to launch, fly, and control multiple UAVs in a limited combat airspace and, additionally, to evaluate their ability to cooperate with networked ground and remote assets to receive and transmit data during realistic operations like target identification (biometrics), target tracking, and area security.

A. CONCEPT OF OPERATIONS

A simulated SOF team with Biometric Collection equipment conducted routine check point operations for suspicious individuals and IED vehicles in a host nation without a reliable database of information on suspected terrorists. A reliable transfer of biometrics data from the check point to the forward operating base (TOC at Camp Roberts) and via the OFDM backbone and VPN to the Biometrics Fusion Center (BFC), was the main concern of the experiment. Connectivity between check point and TOC was accomplished by using the LRV, multiple UAVs, and tethered balloon. TOC directed 4 UAVs (Raven, Pointer, TERN UAV, NPS SUAV) providing surveillance and security flights in the vicinity and searching for a potential IED vehicle.

B. EXPERIMENT ASSETS AND TECHNOLOGIES

The field experimentation was focused on the following areas:

- The performance of the 802.16 OFDM testbed, between the Tactical Operations Center at Camp Roberts and the NPS NOC. The NOC had VPN connectivity with the BFC, USSOCOM, and LLNL. They all provided network monitoring and management, data collection, and situational awareness about the status of the network nodes.
- Biometrics laptops for obtaining and transmitting 4-print and 10-print ID for High Value Target (HVT) identification.
- Light Reconnaissance Vehicle (LRV) as a joint point for the various wireless networks, providing long-haul reach back to the TOC.
- Airspace deconfliction of multiple UAVs in a coordinated surveillance and reconnaissance mission.
- The performance of INTER-4 Tacticomp, which is a ruggedized PDA with VoIP, video and data capability and provides blue force tracking using ITT mesh network connectivity.
- Collaboration and Situational Awareness (SA) Tools.

C. ANALYSIS OF SCENARIO PERFORMANCE

During TNT 06-1, we observed a consistent network connectivity and throughput of OFDM 802.16 backbone between Camp Roberts and NPS. The 802.16 OFDM functioned with high bandwidth and without failure. The link was adequate to stream video and voice over IP, as long as connectivity with TERN UAV and mesh nodes remained. The average response time was about 5 ms (Figure 35).

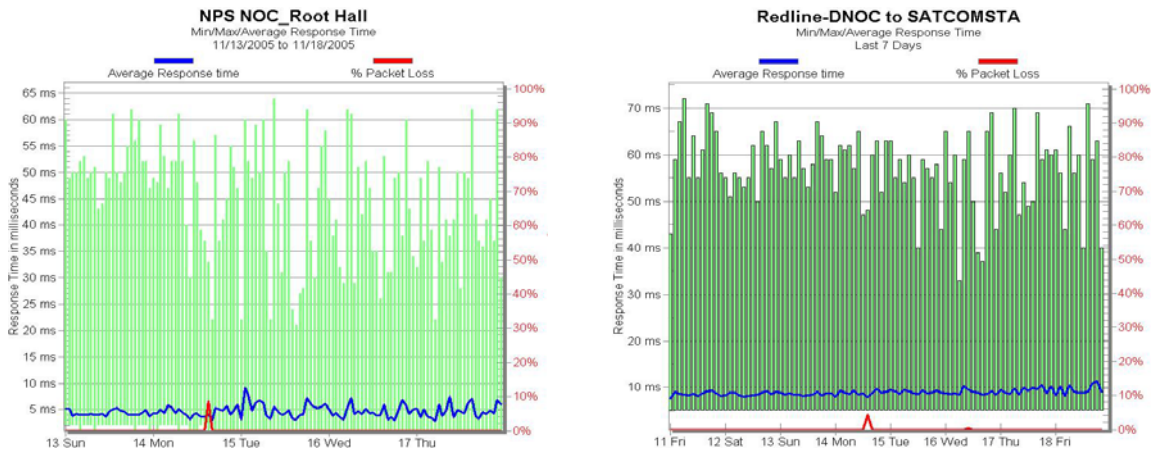


Figure 35. OFDM Backbone Stability

The Light Reconnaissance Vehicle (LRV) operated as a Mobile TOC, used a parabolic antenna, and had the ability to rapidly set-up communication relays between dismounted soldiers and the TOC. The link remained stable and some performance variations were due to location and distance. The Solar Winds monitoring tool displays high throughput (0.6 Mbps), with low average response time, about 5-7 ms (Figure 36).

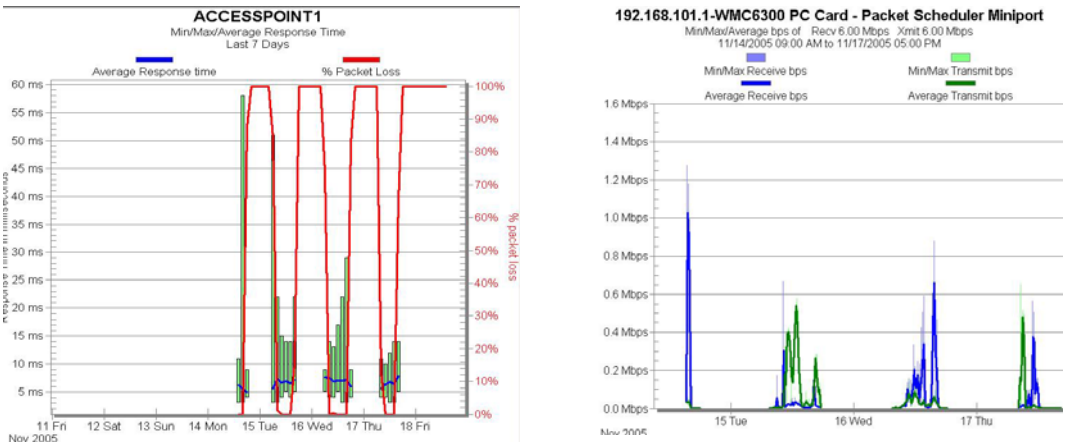


Figure 36. LRV Access Point Performance

The SOF team took digital fingerprints for advanced HVT identification. Fingerprint files are large, around one Mb, and require very large bandwidth to transmit.

The ten fingerprint file was transmitted to the Biometrics Fusion Center and the identification match was received in 6 minutes.

TNT 06-1 tested the viability and stability of the Tacticomps during mission execution. Video from Tacticomps was successfully sent from the Check Point to the TOC using the LRV. From LRV to TOC the link was via the 802.16 backbone. The LRV was functioning as a TOC providing a mobile platform for direct communication between the SOF members. Using Solar Winds software tools, the NOC facilitator was able to monitor the health of each Tacticomp and collect statistics data. Collected data from the Tacticomp showed that when the vehicle was at the farthest point away from the Tacticomp, there was little to no connectivity (Figure 37). TOC recommended reconfiguration of the Tacticomps or movement of the vehicle to acquire stable communications.

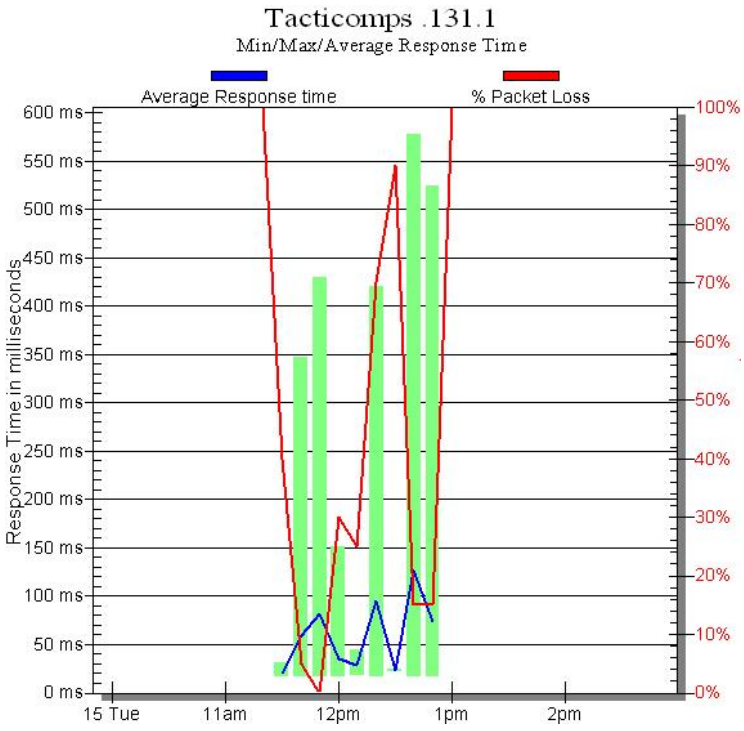


Figure 37. Tacticomp Connectivity

SNMP Real-Time Graphs revealed real-time information on a specific node in the network. For example, Figure 38 is a continuous throughput real-time graph for the wireless joint point on the LRV during data transmission from Tacticomp.

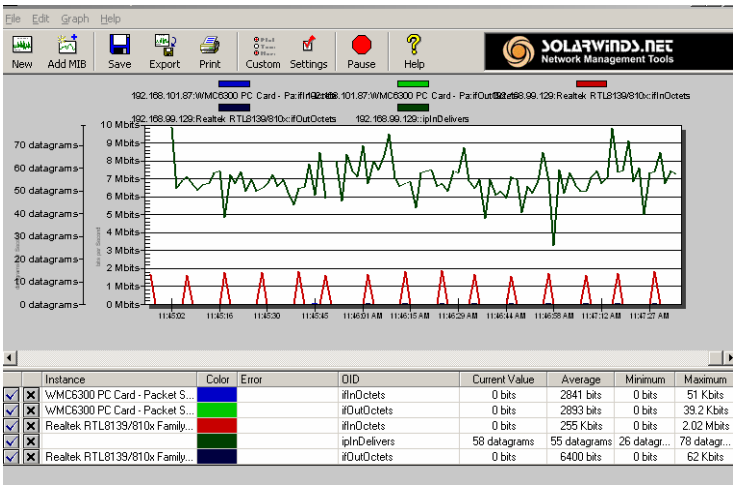


Figure 38. Throughput Real-Time Graph

Collaboration and Situational Awareness (SA) tools were also used providing significant potential for common operational picture of nodal status and operational activity. The NOC was able to view nodes in the field and identify node location via latitude and longitude coordinates (Figure 39).

Figure 39. Situation Awareness During TNT 06-1

Solar Winds provided visibility for the performance of the TERN UAV during mission execution. The health of the network was being monitored both by the NOC at NPS and TOC at CR, so it was important to know the status of a node at any given time, why it went down, why it was dropping packets, and how to resolve the problem. Figure 40 illustrates the response time during transmitted video (10:30) as well as experiment execution (10:00-11:30 and 12:00-13:00).

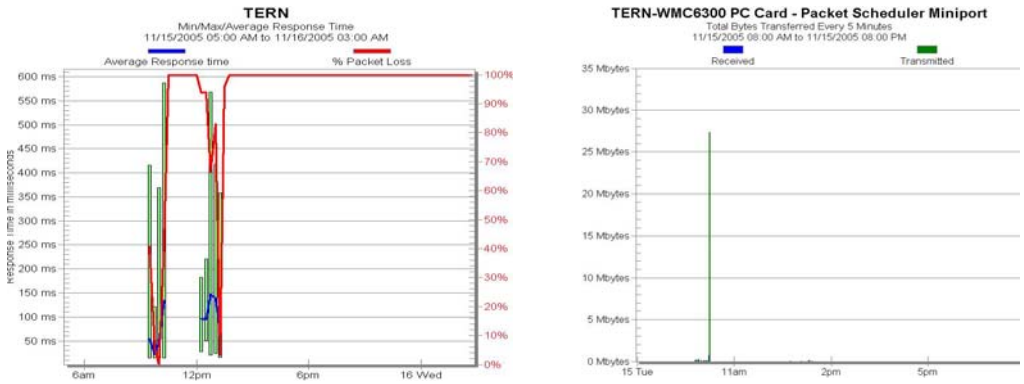


Figure 40. TERN UAV Response Time

Video from TERN UAV (Figure 41) was transmitted to the TOC and the NPS NOC via the 802.16 OFDM backbone and provided the ability to conduct area surveillance during execution of the HVT search mission.

Figure 41. Video From TERN UAV

Another method that increased the situational awareness and the feedback about the status of the network to the NOC was the creation of thresholds and alerts in Solar Winds Orion. The network management software enabled us to receive warnings when a specified threshold had been exceeded and to take preventive actions to support network operations. Figure 42 illustrates the log of triggered alerts when the number of dropped packets from critical network nodes in the mesh topology exceeded a certain threshold.

Triggered Alerts for All Network Devices

TIME OF ALERT	NETWORK DEVICE	NETWORK OBJECT	CURRENT VALUE	ALERT MESSAGE
% Packet Loss				
11/17/2005 04:41 PM	ACCESSPOINT1	ACCESSPOINT1	100 %	Current packet loss for ACCESSPOINT1 is 50 %. Average Response time is 7 ms and is varying from 6 ms to 8 ms.
11/17/2005 01:04 PM	Balloon1	Balloon1	100 %	Current packet loss for Balloon1 is 50 %. Average Response time is 34 ms and is varying from 21 ms to 68 ms.
11/17/2005 01:18 PM	Balloon2	Balloon2	100 %	Current packet loss for Balloon2 is 50 %. Average Response time is 46 ms and is varying from 17 ms to 96 ms.
11/17/2005 09:17 AM	LRV OFDM T6	LRV OFDM T6	100 %	Current packet loss for LRV OFDM T6 is 50 %. Average Response time is 7 ms and is varying from 6 ms to 7 ms.
11/17/2005 09:42 AM	LRV3	LRV3	100 %	Current packet loss for LRV3 is 50 %. Average Response time is 7 ms and is varying from 6 ms to 9 ms.
11/18/2005 11:17 AM	NPS-BORDPAN	NPS-BORDPAN	100 %	Current packet loss for NPS-BORDPAN is 50 %. Average Response time is 5 ms and is varying from 4 ms to 9 ms.
11/17/2005 12:07 PM	Raven2	Raven2	100 %	Current packet loss for Raven2 is 50 %. Average Response time is 5 ms and is varying from 5 ms to 6 ms.
11/17/2005 12:10 PM	Raven3 (Mesh)	Raven3 (Mesh)	100 %	Current packet loss for Raven3 (Mesh) is 50 %. Average Response time is 32 ms and is varying from 19 ms to 65
11/17/2005 12:09 PM	Raven4 (Mesh)	Raven4 (Mesh)	100 %	Current packet loss for Raven4 (Mesh) is 50 %. Average Response time is 24 ms and is varying from 11 ms to 47

Figure 42. Triggered Alerts in Solar Winds Orion

Application servers at CENETIX were important network devices that the NOC monitored during TNT 06-1. Solar Winds provided information and graphs on traffic volume during certain periods. The analysis considered a number of variables such as the average and maximum CPU and memory utilization, most utilized interfaces, error statistics and the periods when traffic rates exceeded a given threshold. For example in Figure 43, send/receive traffic on the network interface of the Solar Winds server was sampled every 15 minutes during the week of the experiment.

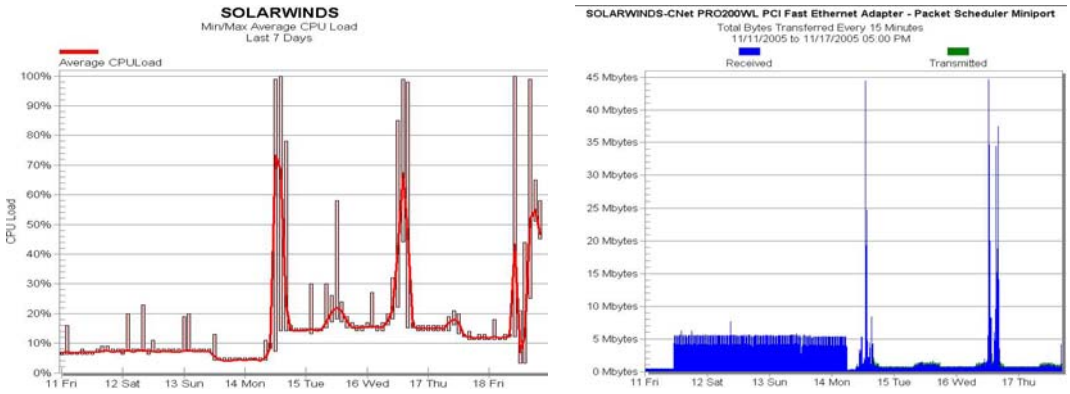


Figure 43. Server CPU Utilization During TNT 06-1

From the graph we can discover and flag the peaks in server utilization. The graph depicts a clear pattern of high CPU utilization on Monday (pre-experiment phase) and on Wednesday during experiment execution. During those days the received traffic (blue color) had reached 45 Mbytes at a time interval of 15 minutes. This happened because, as in TNT 05-4, the server was accepting both SNMP messages from polling all the network nodes and video from TERN UAV, at the same time.

D. TNT 06-1 CONCLUSIONS

During TNT 06-1 some issues were identified relating to the application of advanced technologies in net-centric warfare. On the other hand, the experimentation on 802.16 OFDM networking and network awareness was a success and provided a better understanding of network performance during military operations.

The 802.16 OFDM wireless link again performed well without failures, providing enough bandwidth for streaming video and reach back to the expert resources of the Biometrics Fusion Center.

The combination of collaborative technology, performance management, and fault monitoring provided the desirable situational awareness for most of the network nodes and users at the testbed and allowed NOC personnel to remedy real-time problems arising from configuration and traffic management.

VI. MODELING NETWORK BEHAVIOR

In Chapter IV we developed a baseline for the TNT testbed, based on its structure and performance. One important factor was left to be investigated: the efficiency of critical applications running on the OFDM backbone. The main objectives were to identify the source and destination of network traffic, avoid critical bottlenecks in network design, and characterize the traffic flow by measuring the bandwidth utilization by each major protocol used during TNT experiments. Network efficiency depends on some protocols that create excessive traffic and degrade performance.

Investigation of network efficiency was performed using a protocol analyzer, a performance management tool that captures network traffic and decodes the protocols providing statistics for network load and response time. For our research we used Ethereal because it is a free, open-source protocol analyzer and decodes most major protocols.

Our goal was to discover any bottlenecks in critical applications and other behavioral patterns for applications and system protocols and to identify whether the transmitted packets were delivered successfully with a minimal packet error rate. For that purpose, a hub was connected to the Redline AN-50 at CENETIX lab. The desktop where Ethereal was installed was running Windows XP and was connected to a port of the hub so all traffic through the testbed could be captured. The captured traffic file represents only a small portion of the TNT 06-1 experiment and includes the video transmission from Raven-4.

A. SIMULATION MODELING BY OPNET TECHNOLOGIES

In addition to the performance management tools previously described, there were also simulation and modeling tools to help network administrators test their network performance and design, build a model, and test alternative solutions. There are several network simulators that can be used to model and analyze application traffic. In our modeling we chose OPNET Modeler 11.5 for the following reasons:

- OPNET is a professional environment for modeling, simulation, and performance analysis of wireless and wired networks
- It provides extensive support and documentation materials
- NPS CENETIX maintains an educational license
- Traffic files that have been captured using Ethereal can be inserted into OPNET environment for further analysis and troubleshooting

OPNET Modeler comes with the module Application Characterization Environment (ACE) which has powerful visualization capabilities, enabling network administrators to visualize application behavior from the application trace file captured from the testbed. In addition to the visualization capabilities, ACE provides diagrams with the sources of delay and applies expert knowledge to troubleshoot network problems.

B. EXAMINING TNT APPLICATION TRAFFIC

The file captured with Ethereal was inserted in OPNET ACE. The following diagram (Figure 44) is a high-level depiction of the transaction and shows the total application bytes sent from each tier and who was talking to whom.

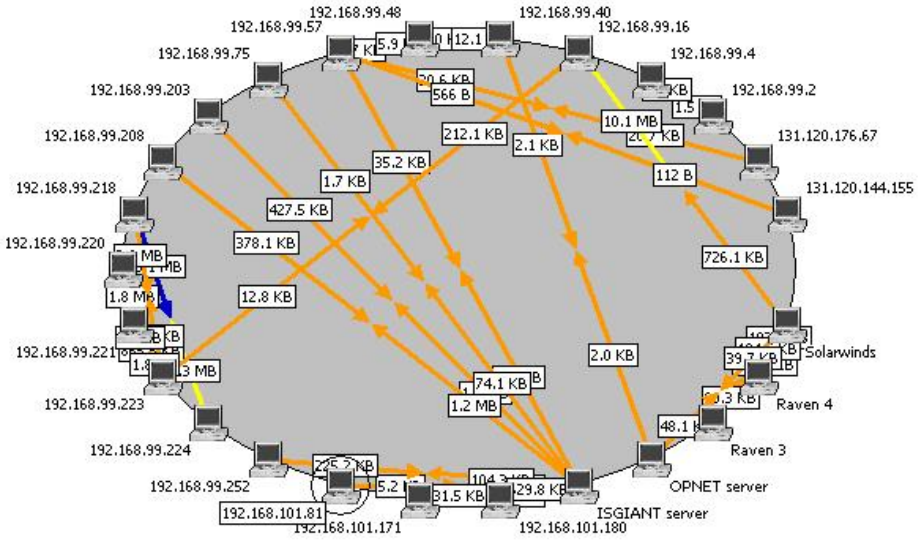


Figure 44. OPNET Tier-Pair Circle

The analysis showed that a share of the total bandwidth was consumed by non-critical nodes and unknown MAC addresses. For that reason, various filters for network nodes were applied to separate the nodes running critical applications (Figure 45).

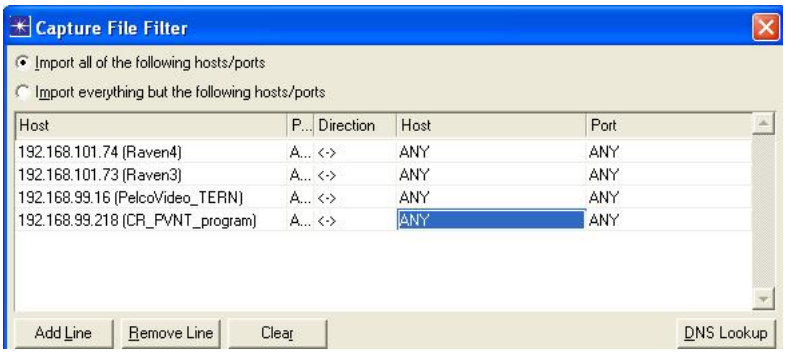


Figure 45. Applying Filter in ACE File

The next step was to specify both the bandwidth and the one way latency for the remote locations. The values that we entered in those fields were 6 Mbytes and 250 ms respectively (Figure 46). ITT Mesh bandwidth is advertised at 6 Mbytes and Solar Winds performance monitor provided the average response time, which was 250 ms, as it is depicted in Figure 47.

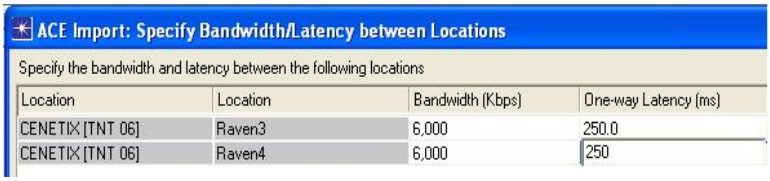


Figure 46. Specify Bandwidth – Latency

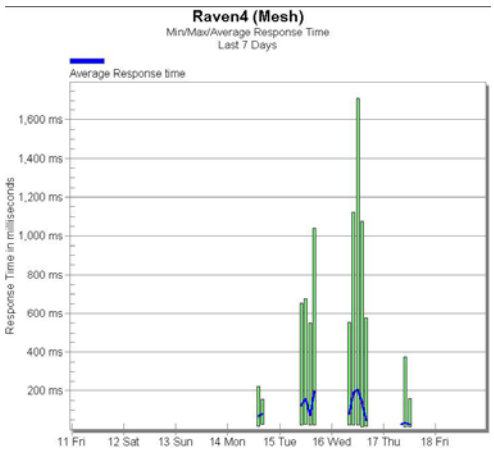


Figure 47. Raven-4 Average Response Time

After we inserted the captured file and specified the required parameters, ACE provided detailed information about the flow of data between the important network nodes and the protocol distribution (Figure 48). From the Data Exchange Chart we observed that for Raven-4, 8 Mbytes of TCP traffic and 990 bytes of SNMP were transmitted. From the Network Chart selection we observed an evenly distributed flow of traffic between network nodes (Figure 49). Blue color represents application payload size greater than 1460 bytes: the video from Raven-4 to Solar Winds. This chart displays the overall flow of application-layer data between tiers focusing on the time interval 0 milliseconds to 560 seconds.

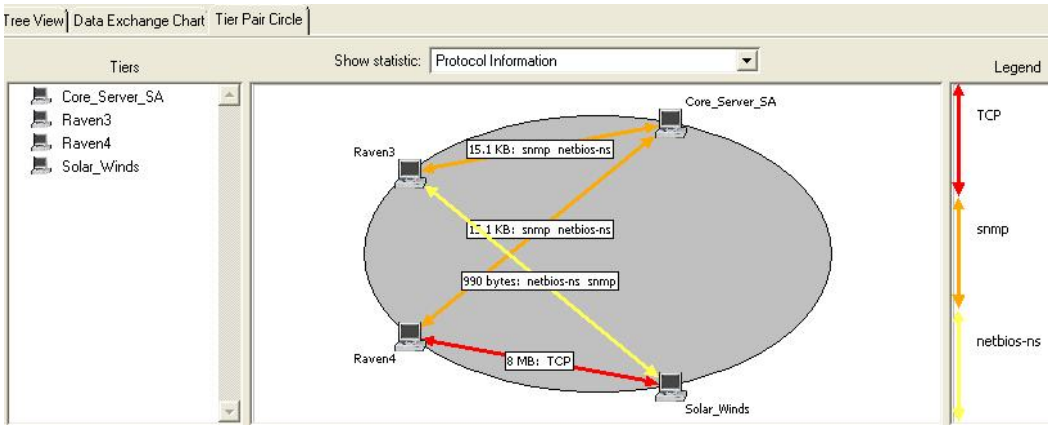


Figure 48. Tier Pair Circle View

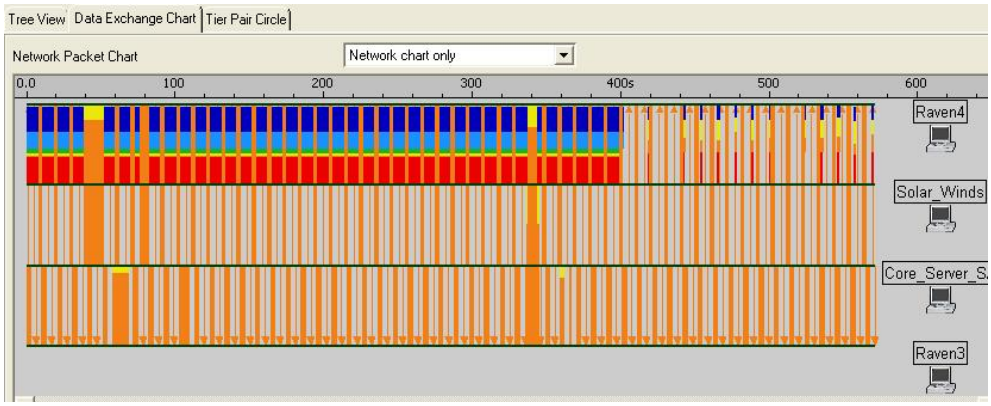


Figure 49. Network Chart Frames

ACE's Application Doctor provided an image with the analysis of the application delays and gave a diagnosis with bottlenecks and potential bottlenecks. Delays are categorized either as Processing Effects or as Network Effects. Application Doctor divided the total application response into four main components and found the major components of delay:

- Tier Processing delay, the total time taken to process the application at each tier
- Latency delay, due to the latency in the network
- Bandwidth delay, caused by the limited bandwidth of the network
- Protocol / Congestion delay, a metric of network restriction to packet flow

For the transaction of our application, 7.4 MB of application data were transferred. According to the diagnosis the delay due to network effects is minimal and only 1.9% is subject to network bandwidth delay. Tier processing delay at Raven-4 was 83.2% and latency delay between Raven-4 and Solar Winds server was 0.6% (Figure 50).

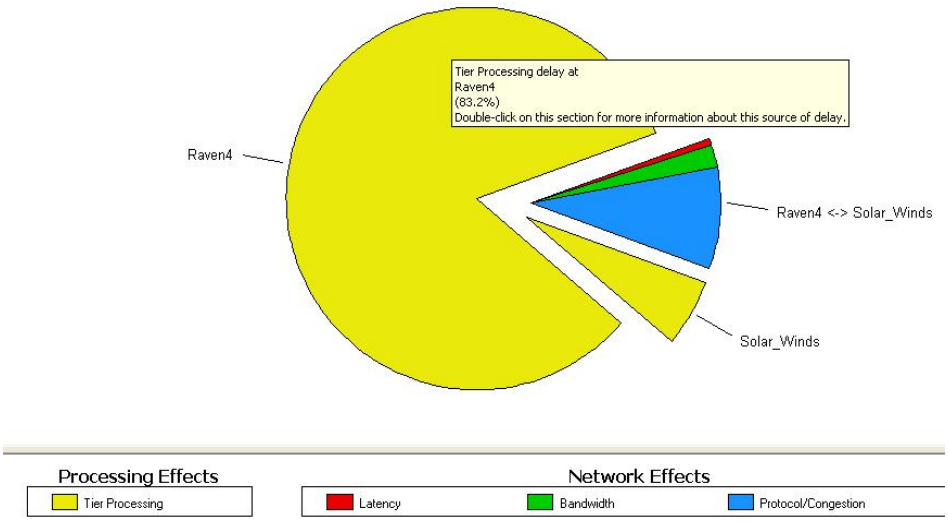


Figure 50. ACE's Summary of Delays

Most of the delay is due to application processing and very little is related to the network. Processing delay is due to file I/O, CPU processing, and memory access. Suggestions provided by OPNET for eliminating the delay include the following:

- Increase the processing speed and capabilities of the tier by increasing the physical memory, increasing the CPU speed, and adding faster disks
- Improve the processing efficiency of the application programs
- Reduce the number of allowed simultaneous connections to limit the load on the tier
- Reduce the load on this tier by sharing its work with additional machines

In addition to the previous network traffic analysis results, OPNET ACE provided statistics with throughput and retransmissions which are considered crucial for the performance of our testbed. The graph at the left in Figure 51 represents the average amount of network data transmitted from the source to the destination tier. This statistic measures network throughput, including all application data and network protocol overhead. Examining the blue line, the traffic from Raven-4 to Solar Winds averages about 250 kbits and has a spike around 430 kbits. The OFDM backbone has an available

bandwidth of at least 6 Mbytes when transmitting and receiving with low RSSI. The graph at the right, shows the losses which seem to be fairly even and minimal.

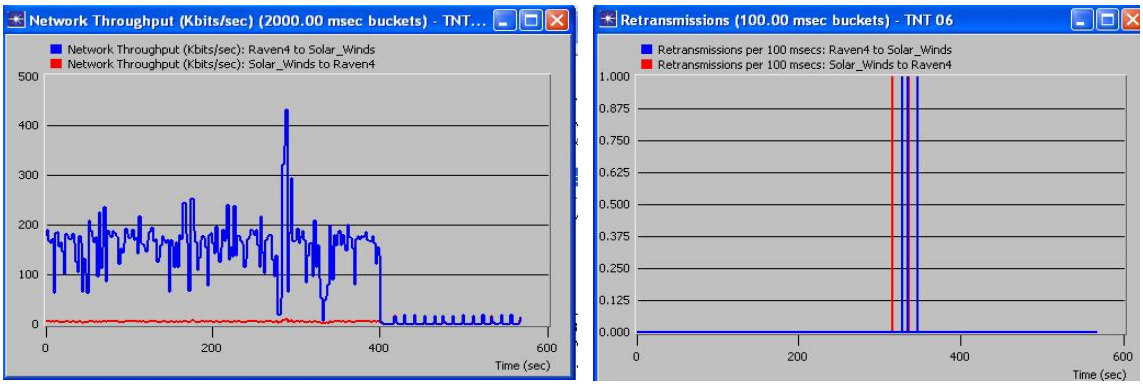


Figure 51. Network Throughput and Retransmissions

The Quick Prediction Tool is mainly concerned with evaluating network performance under different application scenarios by employing "what-if" analysis in order to identify likely problems. The impact of bandwidth and link utilization is the primary reason affecting the overall application response time. Figure 52 illustrates that response time remains constant and application performs better when the link utilization remains lower than 85%.

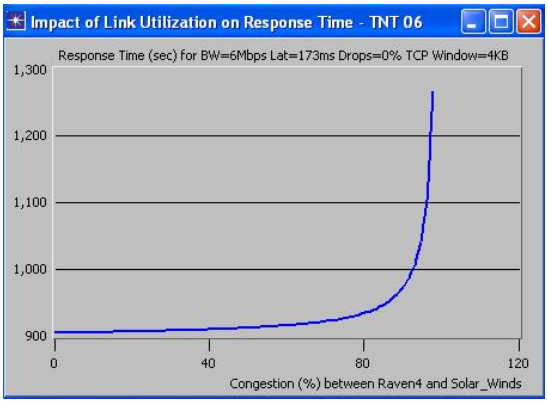


Figure 52. Impact of Bandwidth on Response Time

C. CONCLUSIONS FROM TRAFFIC ANALYSIS

This application analysis was conducted for the first time and was focused on a small portion of the TNT program. In military networks, it is important to ensure that the

quality of service for critical applications is satisfied and new applications will not degrade the performance of existing ones. Traffic was captured while video was transmitted from mesh nodes to the NOC and we picked out only the participating nodes, leaving out all other traffic. The analysis of the network traffic patterns provided delay characteristics for video transmission.

During our study we identified some important aspects. First of all, in order to model the applications of our testbed in OPNET, we needed to take into consideration a lot of parameters, like bandwidth and latency for every node. Ethereal is a powerful protocol analyzer for traffic analysis, but we believe that the use of ACE's capture agents will help in constructing a more accurate application model for Mesh networks. Second, TNT experiments are conducted in a limited time with a lot of network nodes, different emerging technologies, and various applications running simultaneously so there are many unidentified aspects that may influence network behavior.

Overall, with the tools we used and the parameters we specified in ACE, we believe that the analysis reflects the reality of TNT behavior and performance. In essence, no significant end-to-end delays were identified on the OFDM testbed. Most of the delay in application response time is due to application processing and very little is related to the network. The OFDM backbone bandwidth is sufficient and not a constraint for the applications currently in use during TNT experiments.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. OVERVIEW

The ultimate objective of Network Centric Warfare (NCW) is to provide all elements of the GIG with increased connectivity and access to high quality information. For that reason, it requires systems that will provide advanced performance capabilities in terms of bandwidth, quality of information, decision aids, and situational awareness among networked entities. Beyond military operations, the ability to rapidly extend a high bandwidth collaborative environment is essential to the timely response of civil and natural disasters.

The Center for Network Innovation and Experimentation (CENETIX) and the NPS field experimentation program explores the concepts of NCW by evaluating some of the latest technologies and network configurations in order to address problems associated with their transformation into a real operational capability. One of the most important aspects and demanding tasks in network design is to measure network performance and effectiveness.

In this thesis, we have examined the applicability of the 802.16 OFDM wireless technology to support a range of military operations requiring mobility and highly adaptive ad-hoc organization. Three techniques were used to assess the operation of the 802.16 NPS testbed for its quality requirements: Field experimentation scenarios, network performance management tools and modeling tools.

First, the scope of this thesis was to help develop strategies and processes for implementing network management. Network performance patterns at layer 2 and layer 3 were explored as well as their association to critical application performance. We tested the performance using Solar Winds and we saw how situational awareness was provided in a holistic network behavior model. A baseline was conducted to record the state of the OFDM testbed operation over a period of time of more than one year and we investigated the operational guidelines and conditions for the network to support collaborative applications with response times that users would find acceptable. The baseline provided good organization, status monitoring and planning capabilities that will help in

troubleshooting future failures. Our study helped to identify desirable interfaces, recommend metrics for each of them, and different ways to aggregate and present statistical data regarding the performance. Thresholds were set to specific values to generate alarms to inform network operators when a particular situation had occurred. Various reports on the efficiency of the system and its current and previous performance were provided on a daily, weekly, and monthly basis. The final conclusion is that 802.16 OFDM provides reliable performance and high throughput at significant distances.

Second, we have identified critical military applications and diagnosed performance issues. OPNET Modeler ACE let us examine network traffic flow based on application type, source and destination addresses. To determine testbed efficiency, we used Ethereal as a packet analyzer and OPNET ACE for modeling critical application flow. By modeling the traffic flow, we were able to characterize the behavior of the OFDM testbed and quantify network performance. Based upon the knowledge gained from monitoring the testbed and the modeling of traffic flow, future TNT experiments will be able to examine the total bandwidth that a strategic application is consuming and control lower priority traffic that may have an impact in overall performance.

Finally, the responsibilities and the organization of the NPS NOC are presented as well as appropriate policies to monitor and fine-tune network behavior. The Groove Virtual Office and the Situational Awareness (SA) Agent collaborative tools provided the required common operations picture (COP) to the network operators. The combination of well-planned network management and collaborative technology creates a desirable situational awareness so that operators get the right abstraction level of information at the right time, in an easy-to-use format.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

TNT Network Management System has to cope with the heterogeneity of different innovative technologies. It is therefore fundamental to integrate different management stations at every Operational Center (NOC, TOC, and LRV). A plan for data collection should be well defined and each of the management stations will have full control over its network resources. Each of the subnets should be considered as an

autonomous management infrastructure. NPS NOC will be responsible for the OFDM link and performance of the most important critical nodes or joint points. In such a way we will enhance the ability of network management to adjust to frequent topology changes and will minimize operators' management tasks and bandwidth consumption from protocol overhead.

The characterization of critical nodes and the establishment of acceptance criteria before each experiment for specific tests and applications are crucial factors for network management.

During the application modeling phase, we identified a number of issues that should be resolved:

- A more robust modeling analysis can only be achieved by incorporating the OPNET 802.16 model when it will be released
- A more accurate picture of network traffic for the TNT will be produced by using the ACE Capture Agents instead of Ethereal

Since the scope of the field experimentation changes, performance measurements should be repeated at very frequent time intervals and at least twice a year or when new applications are implemented. The creation of simulation scenarios based on specific TNT traffic and performance metrics will help towards a more proactive management of the testbed.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. PERFORMANCE VARIABLES

SYSTEM OBJECTS	
sysDescr	A textual description of the entity – includes full name and version of the system's HW, SW and networking SW
sysObjectID	The vendor's authoritative of the network management subsystem – this value is allocated within the SMI enterprises subtree, for determining what kind of box is been managed
sysUptime	Time since the NW management portion of the system was last re-initialized
sysContact	The contact person of this managed device
sysName	An administratively assigned name for this device
sysLocation	The physical location of this node
sysServices	A value which indicates the set of services this entity offers
INTERFACES OBJECTS	
ifInOctets	Total number of octets received on the interface
ifInUcastPkts	Number of packets delivered from this sublayer to a higher layer which were not addressed to multicast or broadcast
ifInNUcastPkts	Number of packets delivered from this sublayer to a higher layer which were addressed to multicast or broadcast address at this sub layer
ifInDiscards	Number of inbound packets which were chosen to be discarded, even though no errors had been detected to prevent their being deliverable to a higher layer protocol: one possible reason is to free up buffer space
ifInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher level protocol
ifInUknownProtos	Number of packets received via the interface, which were discarded because of an unknown or unsupported protocol
ifOutOctets	Total number of octets transmitted out of the interface
ifOutUcastPkts	Total number of packets that higher level protocols requested be transmitted and which were not addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent
ifOutNUcastPkts	Total number of packets that higher level protocols requested be transmitted and which were addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent
ifOutDiscards	Number of outbound packets which were chosen to be discarded, even though no errors had been detected to prevent their being transmitted: one possible reason is to free up buffer space
ifOutErrors	The number of outbound packets that could not be transmitted because of errors

IP OBJECTS	
ipInReceives	Total number of input datagrams received from interfaces, including those received in error
ipInHdrErrors	Number of input datagrams discarded due to errors in their IP headers (bad check sums, version number mismatch, other format errors)
ipInAddrErrors	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity
ipForwDatagrams	Number of input datagrams for which this entity was not the final IP destination – as a result an attempt was made to find a route to forward them to the final destination
ipInDiscards	Number of input datagrams for which no problem were encountered to prevent their continued processing but which were discarded (for lack of buffer space)
ipInDelivers	Total number of input datagrams successfully delivered to IP user protocols
ipOutRequests	Total number of IP datagrams which local IP user protocols supplied to IP in requests for transmission
ipOutDiscards	Number of output datagrams for which no problem were encountered to prevent their transmission to their destination but which were discarded (for lack of buffer space)
ipOutNoRoutes	Number of datagrams discarded because no route could be found to transmit them to their destination
ipRoutingDiscards	Number of routing entries that were chosen to be discarded even though they are valid: one possible reason could be to free up buffer space for other routing entries
UDP OBJECTS	
udpInDatagrams	Total number of UDP datagrams delivered to UDP users
udpOutDatagrams	Total number of UDP datagrams sent from this entity
SNMP OBJECTS	
snmpInPkts	Total number of messages delivered to the SNMP entity from the transport service
snmpOutPkts	Total number of messages which were passed from the SNMP protocol entity to the transport service
snmpInGetRequests	Total number of SNMP get-Request PDUs which have been accepted and processed from the SNMP protocol entity
snmpOutGetResponses	Total number of SNMP get-Response PDUs which have been generated by the SNMP protocol entity

Table 6. Most Important Performance Variables

LIST OF REFERENCES

3COM, *Simple Network Management Protocol*. http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c15snmp.htm. Last Accessed October 2005.

Aidarous, S., (1998). *Telecommunications Network Management*. New York: IEEE Press.

Anderson, H., (2003). *Fixed Broadband Wireless System Design.* England: John Willey & sons.

Blazevich, R., (2004). *Wireless, Long Haul, Multi-Path Networking: Tranforming Fleet Tactical Network Operations With Rapidly Deployable, Composable, Adaptive Environments.* Master's Thesis, Naval Postgraduate School, Monterey, CA.

Bordetsky, A., Dolk, D., (2002). *Knowledge Management for Wireless Grid Operation Centers.* Proceedings of the 35th Hawaii International Conference on System Sciences.

Callaway, E., (2004). *Wireless Sensor Networks: Architectures and protocols*. New York: Auerbach Publications.

Cisco, *Wireless Technologies*. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/wireless.htm#xtocid14 Last Accessed October 2005.

Jeoun, K., (2004). *The Tactical Network Operations Communications Coordinator in Mobile UAV Networks.* Master's Thesis, Naval Postgraduate School, Monterey, CA.

Gast, M., (2005). *802.11 Wireless Networks, The Definitive Guide, 2nd edition*. Sebastopol, CA: O'Reilly.

Heiskala, J., (2003). *OFDM Wireless LANs: A Theoritical and Practical Guide, 1st edition*. Sams.

Ibe, O., (2002). *Fixed Broadband Wireless Access Networks and Services, 1st edition*. New York: John Wiley & Sons Inc.

IEEE. Standard for Local and Metropolitan Area Networks - Part 16. *Air Interface for Fixed Broadband Wireless Access Systems*. http://www.ieee802.org/16/pubs/80216-2004.html. Last Accessed October 2005.

IEEE Std 802.11-1997. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Institute of Electrical and Electronics Engineers, Inc., New York.

Klopson, J., Burdian, S., (2005). *Collaborative Applications Used in a Wireless Environment at Sea for Coast Guard Law Enforcement and Homeland Security Missions*. Master's Thesis, Naval Postgraduate School, Monterey, CA.

Lambert, (1995). *A Model for Common Operation Statistics*. Request for Comments: 1857, Network Working Group.

Marvin, C., (2005). *802.16 OFDM Rapidly Deployed Network for Near-Real-time Collaboration of Expert Services in Maritime Security Operations*. Master's Thesis, Naval Postgraduate School, Monterey, CA.

McKeller,B., *Network Baselining, Part I: Understanding the Past to Predict the Future* (white paper), Acterna http://www.acterna.com/united_states/technical_resources/white_papers/baselin1.html . Last Accessed July 2005.

McKeller,B., *Network Baselining, Part II: The Big Picture* (white paper), Acterna http://www.acterna.com/united_states/technical_resources/white_papers/baselin2.html . Last Accessed July 2005.

McKeller,B., *Network Baselining, Part III: Focus on the Nodes* (white paper), Acterna http://www.acterna.com/united_states/technical_resources/white_papers/baselin3.html . Last Accessed July 2005.

Network World. *MIBs*. http://www.networkworld.com/details/749.html?def Last Accessed October 2005.

NSA, *Global Information Grid (GIG)*. http://www.nsa.gov/ia/industry/gigscope.cfm?MenuID=10.3.2.2. Last Accessed October 2005.

Olexa, R., (2005). *Implementing 802.11, 802.16 and 802.20 Wireless Networks: Planning, Troubleshooting and Operations.* Oxford, UK: Newnes.

Oppenheimer,P., (2004) Top-Down Network Design, 2nd ed. Indianapolis, Indiana. Cisco Press.

Pentikousis, K., & Acosta, B. *Network Resource Planning*. Available at http://www.cs.stonybrook.edu/~kostas/art/nrp/. Last Accessed October 2005.

Smith, C., (2005). *3G Wireless with 802.16 and 802.11, 1st edition*. New York: McGraw Hill Professional.

Subramanian, M., (2000). *Network Management, Principles and Practice*. New York: Addison Wesley.

Sweeney, D., (2004). *Wimax Operator's Manual: Building 802.16 Wireless Networks, 1st edition.* Berkeley, CA: Apress.

Unger, J., (2003). *Deploying License-Free Wireless Wide Area Networks, 1st edition.* Indianapolis, Indiana: Cisco Press.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

4. Alexander Bordetsky
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Maj (USMC) Carl Oros
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

6. Christoforos Zachariadis
   Hellenic Army General Staff
   Athens, Greece